GRIFFITH COLLEGE DUBLIN

LLM Dissertation Submission Cover Sheet

Student name:	**ESTHER TEH SUE HUI**
Student number:	**3103211**
Dissertation title:	**EVALUATION OF CROSS-BORDER PERSONAL DATA TRANSFER MECHANISMS BETWEEN MALAYSIA AND THE EUROPEAN UNION**
Supervisor's name:	**DENIS HEALY**
Supervisor's signature:	**14th August 2023**

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understand the college's policy on plagiarism and that my dissertation will be checked for plagiarism through TURNITIN. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this dissertation, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this dissertation is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the dissertation has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Signature of student: Esther **Date:** **16th August 2023**

Note to LLM students: You **MUST** submit TWO HARD-BOUND COPIES + A COPY ON MOODLE. You MUST retain the receipt issued to you as proof of submission.

FOR OFFICE USE ONLY:

No. of copies received (please tick):	2 x hard-bound	_____
Confirmation from student that soft copy submitted on Moodle:	Yes	_____
Date:		_____
Received by:	**Name:**	_____
	Signature:	_____

Evaluation of Cross-Border Personal Data Transfer Mechanisms between Malaysia and the European Union

Research dissertation presented in partial fulfilment of the requirements for the degree of
LLM in International Law
(QQI)

Law School, Griffith College Dublin

Esther Teh Sue Hui

2023

CANDIDATE DECLARATION

Candidate Name (please print): ESTHER TEH SUE HUI

I certify that the dissertation entitled: **Evaluation of Cross-Border Personal Data Transfer Mechanisms Between Malaysia and the European Union**

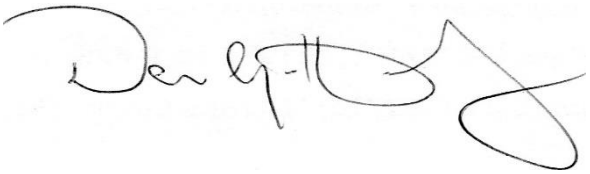
submitted for the degree of: **LLM in International Law**

is the result of my own work and that where reference is made to the work of others, due acknowledgment is given.

Candidate signature: 

Date: 16th August 2023

Supervisor Name (please print): Denis Healy

Supervisor signature: 

Date: 14th August 2023

ACKNOWLEDGMENTS

I extend my gratitude to my supervisor, Denis Healy, for offering invaluable guidance and constructive feedback during the entire course of completing the dissertation.

I am thankful to my beloved husband, Felix, for his unwavering encouragement and for being a dependable sounding board whenever needed.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviations	Meaning
A29WP	Article 29 Working Party
ASEAN	Association of Southeast Asian Nations
BCR	Binding Corporate Rules
Charter	Charter of Fundamental Rights of the European Union
Data Exporter	Controller and/or Processor established in the EU
Data Importer	Controller and/or Processor established in Third Country
Directive	EU Data Protection Directive 95/46/EC
DMF	ASEAN Data Management Framework
CBPDT	Cross-Border Personal Data Transfer
Certification	Certification Mechanism
COC	Code of Conduct
EC	European Commission
EU	European Union
EU-US DPF	EU-US Data Privacy Framework
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
GDPR	General Data Protection Regulation
MCC	Model Contractual Clauses
PCA	Partnership and Cooperation Agreement
PDPA	Personal Data Protection 2010
PDPA-COP	Personal Data Protection Code of Practice
PDPA-Commissioner	Personal Data Protection Commissioner
PDPA Department	Department of Personal Data Protection
PDPA-Ministry	Ministry of Communications and Multimedia Communications of Malaysia
PDPA Regulations	Personal Data Protection Regulations
PDPA Standards	Personal Data Protection Standard 2015
PDPA Whitelist Order	Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017
PDP	Personal Data Protection
SCC	Standard Contractual Clause
SCC EU	Standard Contractual Clauses for Transfer Within EU/EEA
SCC Third Country	Standard Contractual Clauses for Transfer of personal data to Third Countries
Trading Partners	EU and Malaysia
TFEU	Treaty of the Functioning of the European Union
UK	United Kingdom
US	United States
US Executive Order	Executive Order 14086 ‘Enhancing Safeguards for US Signals Intelligence Activities
US Review Court	US Data Protection Review Court

ABSTRACT

In this paper, the author analysed the diverse mechanisms of cross-border personal data transfers under the European Union General Data Protection Regulation ("GDPR"). This paper further considered the suitability of adopting these mechanisms to the judicial landscape of Malaysia, including the Personal Data Protection Act 2010 ("PDPA"), by comparing the PDPA against the GDPR. In this dissertation, it was shown that the PDPA bears resemblance to the GDPR to a certain extent. This paper further revealed that the disparity between the PDPA and the GDPR was found to be the impediment of the PDPA in adopting cross-border personal data transfers mechanisms, which presented a potential trade hindrance in the advanced trade partnership between Malaysia and the European Union through their Partnership and Cooperation Agreement. The author proposed that the PDPA be amended to address the impediments portrayed in the PDPA to strengthen its personal data protection framework, facilitate the adoption of the cross-border personal data transfers mechanisms to the PDPA and to enhance the appeal of Malaysia as a global trading partner.

[A] INTRODUCTION

A1. EU-Malaysia Trade Relations: Milestone Achievement

Malaysia, a prominent member of the Association of Southeast Asian Nations ("**ASEAN**") had formally signed and entered into a Partnership and Cooperation Agreement ("**PCA**") on the 14th of December 2022 with the European Union ("**EU**"), an economic and political coalition made up of 27 countries.[1] The PCA which is the first bilateral trade agreement between the EU and Malaysia ("**Trading Partners**") materialised after a span of over ten years since the first round of negotiations to explore a trading partnership in October 2010.[2] The PCA denotes a remarkable milestone between the Trading Partners as it reflects their commitment to foster trade and economic growth in diverse facets of the partnership in a non-exhaustive manner, i.e. human rights, environment, science and technology.[3] A non-legislative motion for a resolution was adopted by the European Parliament on the 14th of June 2023 pertaining to the draft European Council decision on the PCA.[4]

Derived from the data presented by the European Commission ("**EC**"), the trade relations between the Trading Partners can be succinctly represented as follows: the EU is Malaysia's fourth largest trading partner, whilst Malaysia is the third largest trading partner of the EU within the ASEAN region.[5] Prior to the formalisation of the PCA, the trade in goods between

---

[1] Directorate-General for Communication (European Commission), *The European Union: What it is and what it does* (Publications Office of the European Union 2022) 7; European External Action Service (EEAS) Press Team, 'EU-Malaysia Relations' (*European Union External Action*, 13 January 2023) <https://www.eeas.europa.eu/sites/default/files/documents/EU-Malaysia%20factsheet.pdf> accessed 15 August 2023; Council of the EU, 'Indo-Pacific: The European Union and Malaysia sign Partnership and Cooperation Agreement' (*European Council*, 14 December 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/14/indo-pacific-the-european-union-and-malaysia-sign-partnership-and-cooperation-agreement/#:~:text=The%20Partnership%20and%20Cooperation%20Agreement,that%20started%20in%20October%202010> accessed 15 August 2023.

[2] Framework Agreement on Partnership and Cooperation between the European Union and its member states, of the one part, and the Government of Malaysia, of the other part 11732/22 (Brussels, 3 October 2022) <https://data.consilium.europa.eu/doc/document/ST-11732-2022-INIT/en/pdf> accessed 15 August 2023.

[3] European Parliament non-legislative resolution of 14 June 2023 on the draft Council decision on the conclusion, on behalf of the Union, of the Framework Agreement on Partnership and Cooperation between the European Union and its Member States, of the one part, and the Government of Malaysia, of the other part (11714/2022 – C9-0430/2022 – 2022/0221M(NLE)) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0234_EN.html> accessed 15 August 2023; Ministry of Foreign Affairs Malaysia, 'Malaysia and the European Union Inked the Partnership and Cooperation Agreement 14 December 2022, Brussels, Belgium' (*Ministry of Foreign Affairs Malaysia*, 15 December 2022) <https://www.kln.gov.my/web/guest/-/malaysia-and-the-european-union-inked-the-partnership-and-cooperation-agreement-14-december-2022-brussels-belgium> accessed 15 August 2023.

[4] European Parliament, 'EU-Malaysia Partnership and Cooperation Agreement' (*Legislative Observatory European Parliament*, 14 June 2023) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1747973&t=d&l=en> accessed 15 August 2023.

[5] EEAS Press Team (n 1).

the Trading Partners in 2022 amounted more than €50 billion, whilst in 2021, the value of trade in services between them amounted to almost €7.6 billion.[6] The fruition of the PCA, as the author observes, will increase the trading opportunities between the Trading Partners as it encompasses a broad range of aspects mentioned, including the focus of this paper which is on personal data protection ("**PDP**").[7] This is bolstered by the endeavours presented by Malaysia in its Digital Economy Blueprint 2021 to advance the digital economy in the cross-border trade aspects for the growth of the nation.[8] By means of the relationship forged between the Trading Partners, the author foresees the anticipated outcome is that the EU will impact or influence Malaysia in its development be it in the regulatory, political or commercial aspects, to a varying degree.[9] For instance, the jurisprudence on PDP which Malaysia could draw inspiration and benefit from the EU legal framework, which will be elucidated in this paper.

A2. Interconnection of Trade and Personal Data

The expansion of global trade cultivated the exponential increase in the sales of goods and services via straightforward online transactions, all achieved within a single click, thereby showcasing the interdependence of digital trade with cross-border personal data transfers ("**CBPDT**").[10] The author considers this to be an eminent factor to promote international trade. Federica Velli opines that such interdependence demonstrates prominence to a degree that personal data processing activities have now turned into an 'indispensable aspect of providing competitive services'.[11] The significance of personal data has rapidly transitioned from a mere personal property of an individual to being utilised as a monetisation tool for commercialisation activities.[12]

---

[6] European Commission, 'Malaysia: EU Trade relations with Malaysia: Facts, figures and latest developments' (*European Commission*) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/malaysia_en> accessed 15 August 2023.

[7] Ayman Falak Medina, 'The European Union and Malaysia Sign Partnership and Cooperation Agreement' (*Asean Briefing*, 30 January 2023) <https://www.aseanbriefing.com/news/the-european-union-and-malaysia-sign-partnership-and-cooperation-agreement/> accessed 15 August 2023.

[8] Economic Planning Unit, Prime Minister's Department, 'Malaysia Digital Economy Blueprint' (Government of Malaysia, February 2021) <https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf#page=55> accessed 15 August 2023.

[9] Md Toriqul Islam and Mohammad Ershadul Karim, 'Extraterritorial Application of The Eu General Data Protection Regulation: An International Law Perspective' (2020) 28(2) IIUM Law Journal 531, 540.

[10] Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade' (2020) 10 International Data Privacy Law 201, 201.

[11] Federica Velli, 'The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements' (2019) 4(3) European Papers 881, 881 <https://doi.org/10.15166/2499-8249/325> accessed 15 August 2023.

[12] Beate Roessler, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy' in Beate Roessler and Dorota Mokrosinska (eds), Social Dimensions of Privacy: Interdisciplinary Perspective (Cambridge University Press, Cambridge 2015) 148.

Whilst this appears to be favourable, the author asserts that trade globalisation fostered by monetisation of personal data exposes data subjects to risks as there are conspicuous likelihood of data infringement and violation of rights of data subjects. To conceptualise these observations, the EU pivoted its focus on two conflicting spectrums, as evidenced through its policies. On one hand, the EU commits to promote international trade law and on the other hand, the EU seeks to uphold the fundamental right of individuals on personal data protection.[13] It is apparent that to favour one is to undermine the other. This posed a challenge to converge both the spectrums, however, there are international agreement established to shift the equilibrium, for instance, the General Data Protection Regulation ("**GDPR**")[14] and its antecedent, the EU Data Protection Directive ("**Directive**")[15] which permits unrestricted movement of personal data when enforced.[16]

A3. Aims and Objectives of Research Paper

The focal point of this research paper is to evaluate the various mechanisms of CBPDT introduced by the GDPR and consider adoption of the same within the judicial landscape of Malaysia, including the Personal Data Protection Act 2010 ("**PDPA**"). On a parallel note, the author intends to explore, by way of comparative study, the operation of data protection regime in Malaysia, through its PDPA and the EU, through its prestigious GDPR and assess whether there are any aspects that the PDPA could incorporate and model after the GDPR to facilitate the adoption of the CBPDT mechanisms. The other aims and objectives of this paper encompass the outline of the general framework and the extent of applicability of both the data protection regimes [***Chapter 1, Chapter 2***], review the legal position taken by the PDPA and the GDPR specifically on CBPDT [***Chapter 3***], examine the mechanisms of the CBPDT in each jurisdiction [***Chapters 4 to 6***], make a broad comparison between both data protection framework and identify if there are any trade impediments depicted in the PDPA [***Chapter 7***].

---

[13] Svetlana Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities' (2020) 21 Journal of World Investment & Trade 881, 883.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 ("**GDPR**").

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ("**Directive**").

[16] Graham Greenleaf, 'Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains' in Dan Jerker B Svantesson and Dariusz Kloza (eds), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy (Intersentia 2018) 181-212.

Towards this end, the author aspires to analyse the findings acquired and present recommendations to address the research question.

A4. Research Methodologies

To achieve the aims and objectives set forth above, the author will utilise the desk-based research in preparation of this paper, comprised of three research methodologies namely doctrinal approach, comparative analysis, and socio-legal analysis. The doctrinal approach necessitates the detailed comprehension of prevailing legal position in PDP in both jurisdictions, particularly a review of the primary legislation, the PDPA and the GDPR. Additionally, the author will utilise secondary sources such as academic journals, official publications from relevant government authorities, EU guidelines and books. A comprehensive analysis of the PDPA and the GDPR is highly required to appreciate a clearer understanding on PDP rights particularly its approach on CBPDT, and whether there exist any established mechanisms to guarantee that the same level of protection is maintained outside its jurisdiction.

Further, the author will employ the comparative analysis to compare the two different jurisdictions in their similarities and differences between the approach taken by Malaysia pertaining to movement of personal data outside Malaysia in comparison to the EU's take on the same. The author intends to evaluate the PDP in Malaysia against EU as the GDPR is a world leading PDP framework known for its inclusiveness and has extraterritorial effect premised on the EU fundamental right to ensure data protection rights of individuals are upheld at all times.[17] In the same vein, the author opines that the PDPA is, at its outset, a comparatively lenient framework with various limitations which consequently results in the PDPA being a deficient legislation in the global digital age.[18] As such, the author submits that the PDPA could benefit by deriving ideas from the GDPR to promote recognition of PDP and to elevate the standards of PDP rights for individuals.[19] The comparison would benefit Malaysia primarily to ascertain the gaps between existing frameworks particular in its CBPDT and suggests

[17] European Data Protection Supervisor, 'The History of the General Data Protection Regulation' (*European Data Protection Supervisor*) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,as%20law%20across%20the%20EU> accessed 15 August 2023; Greenleaf, 'Free Trade Agreements' (n 16) 181-212.

[18] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020 Review of Personal Data Protection Act 2010 (Act 709)' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf> accessed 15 August 2023.

[19] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18).

mitigating efforts to reduce disparity thereby fortifying the trade relationship between the two jurisdictions.

Lastly, the author finds it befitting to carry out an analysis from the socio-legal aspect which is feasible to evaluate the practical application of the law as there are external influence closely intertwined with law. The author will evaluate the PDP legislation in each jurisdiction and assess its strength and weaknesses in practice. One of the remarkable elements which heavily influence the law is the trade aspects given the strong connection between international trade law and PDP right which have an impact on one another. Assessment of these aspects are essential as CBPDT promotes economic growth and fosters international relations.[20] Another essential element would be the assessment of the position and approach adopted by policy makers in each jurisdiction and in doing so, the author will rely on official governmental publications, news articles and academic commentaries. This paper will now explore the legal position of PDP in Malaysia.

[20] Yakovleva (n 13) 882.

[B] CHAPTER 1: PERSONAL DATA PROTECTION RIGHTS IN MALAYSIA

1.1 Framework of the Malaysian PDPA

The PDPA was enacted on the 2nd of June 2010, and commenced operation on the 15th of November 2013 along with several subsidiary legislations to supplement the PDPA.[21] For instance, the Personal Data Protection Regulations 2013 ("**PDPA Regulations**"),[22] regulations governing registrations of data user and sector classification of data user,[23] and appointments of Personal Data Protection Commissioner ("**PDPA-Commissioner**"). Historically, the PDPA was a legislative framework which derived inspiration from the United Kingdom ("**UK**") and the EU, such as the Directive which was introduced by the EU policymakers at the initial phase when internet was still in its 'infancy'.[24] Although the Directive was subsequently superseded by the GDPR, the PDPA preserved the provisions albeit the technological progression and advancement in the 21st century. It is however noteworthy that the PDPA is the first data protection legislation within the ASEAN region.[25]

As an overview, the PDPA is a framework consisting of 146 provisions, segregated into eleven different Parts aimed to safeguard the rights of individuals pertaining to their personal data.[26]

---

[21] Personal Data Protection Act 2010 Act 709 ("**PDPA**"); Attorney General's Chambers of Malaysia, 'Personal Data Protection Act 2010' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-detail.php?act=709&lang=BI&date=15-06-2016#timeline> accessed 15 August 2023; Attorney General's Chambers of Malaysia, 'Appointment of Date Coming into Operation' (*Federal Legislation Portal of Malaysia)* <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(B)%20464/2013> accessed 15 August 2023; Nurkhairina Binti Noor Sureani and others, 'The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia' (2021) 6 Malaysian Journal of Social Sciences and Humanities 488, 489; Graham Greenleaf, 'ASEAN data privacy developments 2014-15' (2015) 134 Privacy Laws & Business International Report, 9-12; Graham Greenleaf, 'Malaysia: ASEAN's first data privacy Act in force' (2013) University of New South Wales Law Research Paper No. 12/2014, 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2404893> accessed 15 August 2023.

[22] PDPA, Division II of Part II; Personal Data Protection Regulations 2013 PU (A) 335/2013 ("**PDPA Regulations**"); Attorney General's Chambers of Malaysia, 'Personal Data Protection Regulations 2013' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20335/2013> accessed 15 August 2023.

[23] PDPA, Division III of Part II; Personal Data Protection (Class of Data Users) Order 2013 PU (A) 336/2013; Attorney General's Chambers of Malaysia, 'Personal Data Protection (Class of Data Users) Order 2013' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20336/2013> accessed 15 August 2023.

[24] Deepak Pillai and Yong Shih Han, 'The Privacy, Data Protection and Cybersecurity Law Review: Malaysia' in Alan Charles Raul (9th edn), The Privacy, Data Protection and Cybersecurity Law Review (Law Business Research Ltd 2022) 293; Robert Walters, Leon Trakman and Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (Springer 2019) 199; European Data Protection Supervisor, 'The History of the General Data Protection Regulation' (n 17); Zuryati Mohamed Yusof, 'The Malaysian Personal Data Protection Act 2010: A Legislation Note' (2011) 9 New Zealand Journal of Public and International Law 119, 130.

[25] Abu Bakar Munir, 'Malaysia's Data Protection Law' in Simon Chesterman (ed), *Data Protection Law in Singapore* (Academy Publishing 2014) ch 7.4; Greenleaf, 'Malaysia: ASEAN's first data privacy Act in force' (n 21) 2.

[26] PDPA.

This paper is not intended to set out all the provisions contained therein, however, the author will guide readers through specific provisions which are crucial to examine. For instance, the preliminary provisions on the application of the PDPA under sections 1 to 4;[27] PDP principles under sections 5 to 12;[28] data subject rights under sections 30 to 44;[29] and miscellaneous provisions.[30] It is pertinent to note that whilst the PDPA contains legal terminology similar to the GDPR, there is one particular difference noteworthy at this juncture, i.e. the use of "data user" by the PDPA as compared to "controller" by the GDPR. For purposes of this paper, there will be an interchangeable use of "data user" or "controller" depending on the context in which it is referred to.

1.2 Scope of Application of the PDPA

The PDPA applies only to the processing of personal data in the context of commercial transactions to any person who processes or has control over the processing, irrespective of the establishment.[31] Appointment of a representative in Malaysia is required for establishments outside Malaysia.[32] The PDPA defines commercial transactions as 'any transaction of a commercial nature, whether contractual or not' and covers a broad spectrum of transactions including sale of goods and provision of services, whether in person or through online transactions.[33] However, this excludes any credit reporting activities undertaken by the statutory credit reporting agencies.[34]

It is worth highlighting that the PDPA explicitly excludes the processing of personal data conducted by the government authorities of Malaysia.[35] Unless there is clear intention for processing of personal data in Malaysia, the PDPA has no applicability over processing of personal data carried outside Malaysia .[36] The exclusion list extends to personal data processing activities by individuals for personal or household affairs, investigation purposes, regulatory functions and compliance with court orders.[37]

[27] PDPA, pt I.
[28] PDPA, Division I of Part II.
[29] PDPA, Division 4 of Part II.
[30] PDPA, pt X.
[31] PDPA, section 2(1); PDPA, section 2(2).
[32] PDPA, section 2(3); PDPA, section 2(4).
[33] PDPA, section 4; Walters, Trakman and Zeller (n 24) 200.
[34] PDPA, section 4.
[35] PDPA, section 3.
[36] ibid.
[37] PDPA, section 45.

1.3 Current Legal Position of Data Protection in Malaysia

As a brief background, the Department of Personal Data Protection of Malaysia ("**PDPA Department**") is the department responsible to oversee the implementation and enforcement of the PDPA under the Ministry of Communications and Multimedia Communications ("**PDPA-Ministry")** which is established in 2011.[38] The PDPA-Commissioner is appointed by and is accountable to the PDPA-Ministry.[39]

To derail momentarily, the PDPA Department had on the 15th of December 2022 issued a general code of practice which is legally binding on data user forums to promote adherence of the PDPA and subsidiary legislations.[40] It is important to note that the general code applies only to classes of data users which are not bound by any specific code of practice issued earlier or have yet to provide any sectoral code of practice.[41] The PDPA had earlier issued several sectoral code of practices tailored to individual sectors such as banking and financial,[42] insurance[43] and healthcare industry[44].[45] All the codes of practice issued pursuant to the PDPA shall be

[38] The Government of Malaysia, 'Personal Data Protection Act' (*The Government of Malaysia Official Gateway*) < https://www.malaysia.gov.my/portal/content/654> accessed 15 August 2023; Department of Personal Data Protection, 'Introduction' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/about-us/organization-profile/introduction/?lang=en> accessed 15 August 2023.

[39] PDPA, section 4; PDPA, section 47; Ministry of Communications and Digital, 'Department and Agency Directory' (*Official Portal of Ministry of Communications and Digital*) <https://www.kkd.gov.my/en/directory-and-contact-us/direktori-jabatan-agensi> accessed 15 August 2023.

[40] PDPA, section 23; Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (*Official Portal of Department of Personal Data Protection*, 15 December 2022) 5 <https://www.pdp.gov.my/jpdpv2/assets/2023/01/28.12.2022-FINAL-PRINTING-COP-BI.pdf> accessed 15 August 2023.

[41] PDPA, section 23; Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 5.

[42] Department of Personal Data Protection, 'Personal Data Protection Code of Practice for the Banking and Financial Sector' (*Official Portal of Department of Personal Data Protection*, 19 January 2017) <https://www.pdp.gov.my/jpdpv2/tata_amalan/personal-data-protection-code-of-practice-for-the-banking-and-financial-sector/> accessed 15 August 2023.

[43] Department of Personal Data Protection, 'Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia' (*Official Portal of Department of Personal Data Protection*, 23 December 2016) <https://www.pdp.gov.my/jpdpv2/tata_amalan/code-of-practice-on-personal-data-protection-for-the-insurance-and-takaful-industry-in-malaysia/> accessed 15 August 2023.

[44] Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/tata_amalan/the-personal-data-protection-code-of-practice-for-private-hospital-eng/> accessed 15 August 2023.

[45] Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 5; Department of Personal Data Protection, 'Tata Amalan *(Code of Practice)*' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/tata_amalan/> accessed 15 August 2023.

collectively referred as "**PDPA-COP**". This paper will further elaborate the operation of PDPA-COP in ***Chapter 5.4***.

The PDPA-Ministry announced in the first half of 2023 that there is an ongoing study by the PDPA Department to review and consider additional amendments to the PDPA intended to enhance the data protection security to prevent any fraudulent use of personal data.[46] This is a continuation of the PDPA-Ministry's initiatives back in February 2020 whereby the PDPA-Department issued a public consultation to re-examine the PDPA and identified 22 areas for study and modifications.[47] The PDPA-Ministry announced that five proposed areas for improvement were incorporated to the draft bill expected to be tabled in the Malaysian Parliament in October 2022, however it was put on hold to pave way for the general election which took place in Malaysia in November 2022.[48]

The announcement made by the PDPA-Ministry in January 2023 arises from the newly appointed cabinet of Malaysia on the proposed additional areas for improvement which concerns the need for data user to issue mandatory notifications arising from personal data breach and the increase in the fines and/or penalties against perpetrators found liable for mishandling of personal data.[49] It is not known at the time of writing what are the specific areas to be tabled in parliament as the legislative amendment is anticipated by the end of 2023, or early 2024.[50] Notwithstanding the lack of clarity at this juncture, the author observes that the PDPA-Ministry has taken a relatively consistent approach in acknowledging the exorbitant surge in personal data breaches in Malaysia in recent years hence, the author submits that a

---

[46] Digital Watch, 'Revision of Malaysia's Personal Data Protection Act 2010 is needed, Minister of Communications and Digital Communications claims' (*Digital Watch*, 18 June 2023) <https://dig.watch/updates/revision-of-malaysias-personal-data-protection-act-2010-is-needed-minister-of-communications-and-digital-communications-claims> accessed 15 August 2023; MalayMail, 'Fahmi: Amendments to Personal Data Protection Act to be tabled in Parliament by year end', (The MalayMail, 25 January 2023) <https://www.malaymail.com/news/malaysia/2023/01/25/fahmi-amendments-to-personal-data-protection-act-to-be-tabled-in-parliament-by-year-end/51871> accessed 15 August 2023.

[47] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18).

[48] Christopher & Lee Ong, 'Latest Update on the Proposed Amendments to the Personal Data Protection Act 2010' (*Christopher & Lee Ong*, August 2022) <https://www.christopherleeong.com/media/5004/2022-08_clo_pdpa-amendments-oct-2022.pdf> accessed 15 August 2023; Baker McKenzie, 'Data Privacy and security' (Baker McKenzie) <https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/apac/malaysia/topics/data-privacy-and-security> accessed 15 August 2023.

[49] MalayMail (n 46).

[50] Bernama, 'Fahmi: Personal data protection act needs amending to avoid data abuse' (New Straits Times, 18 June 2023) <https://www.nst.com.my/news/nation/2023/06/921606/fahmi-personal-data-protection-act-needs-amending-avoid-data-abuse> accessed 15 August 2023; Albert Lim, 'Capitalize on technology to strengthen your data security' (The Star, 23 June 2023) <https://www.thestar.com.my/business/business-news/2023/06/23/capitalise-on-technology-to-strengthen-data-security> accessed 15 August 2023.

review of the PDPA is necessary given its inefficacy to be elaborated in ***Chapter 7.2*** to cater to demands in digital age.[51]

The advancement of the EU-Malaysia trade partnership, the prevalence of data breaches and the interrelation of personal data and digital trade are supporting factors for the re-examination of the PDPA and the author advocates for the policymakers to consider appropriate changes to accord a stronger data protection regime to safeguard individuals' rights to personal data protection.[52] Simultaneously, this prepares Malaysia, from an economic perspective, to be an unwavering trading partner of EU with shared values and visions from the perspective of PDP.[53] Where this can be achieved, the author views that the standards of the PDPA could rise above to a level equivalent to or comparable to its formidable counterpart, the GDPR, enabling it to be aligned with the EU principles in recognition of the fundamental PDP rights mandated by the Charter of the Fundamental Rights ("**Charter**").[54] The author will now provide a brief synopsis of the GDPR.

[51] BBC, 'Malaysian data breach sees 46 million phone numbers leaked' (*BBC*, 31 October 2017) <https://www.bbc.com/news/technology-41816953> accessed 15 August 2023; Rahimi Yunus, 'Almost 200% increase in data breach attacks since 2018' (*The Malaysian Reserve*, 17 October 2019) <https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/> accessed 15 August 2023; Aaron Raj, 'A hole or a mole in Malaysian government agencies as another database leaked?' (*TechWire Asia,* 18 September 2022) <https://techwireasia.com/2022/09/a-hole-or-a-mole-in-malaysian-government-agencies-as-another-database-leaked/> accessed 15 August 2023.
[52] MalayMail (n 46).
[53] ibid.
[54] Charter of Fundamental Rights of the European Union [2012] OJ C326/391 ("**Charter**"), Article 8.

[C] CHAPTER 2: DATA PROTECTION RIGHTS IN THE EU

2.1 Framework of the EU GDPR

The GDPR which was directly applicable to and has direct effect across the EU Member States from the 25th of May 2018 pursuant to Article 288 of the Treaty of the Functioning of the European Union ("**TFEU**"), was introduced as a regulatory framework to govern the processing of personal data concerning natural persons.[55] The EU policymakers introduced the GDPR to meet the objectives of the Charter and TFEU and to uphold the fundamental rights of EU citizens in PDP.[56] The birth of the GDPR to supersede the Directive was necessitated by the 'patchwork in diverse privacy protection mechanisms' caused by the Directive, hence it was unable to accord uniform application of the PDP regime across the EU member states.[57] It is noteworthy that the GDPR was incorporated into the European Economic Area ("**EEA**") Agreement on the 6th of July 2018.[58] The adoption of the GDPR symbolises the fact that the protection accorded under the GDPR extends to EEA region to include countries such as Iceland, Liechtenstein and Norway.[59]

The GDPR is a legislative framework with 99 articles accompanied by 173 recitals which sought international recognition as 'one of the greatest achievements in recent years' tailored to accommodate the technology advancement.[60] The author views the GDPR as a paragon for being a comprehensive legislative framework which inspired other countries globally to follow pursuit to introduce GDPR-like data protection legislation.[61] Some countries such as Norway and Switzerland had harmonized their domestic data protection legislation to conform to the GDPR due to its broad application which significantly impacted the way personal data is managed within and outside of EU.[62] An academician commented that the GDPR is influential

---

[55] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/1 ("**TFEU**")
[56] Charter, Article 8(1); TFEU, Article 16(1); GDPR, recital 1; GDPR, art 99.
[57] Islam and Karim (n 9) 533 - 534.
[58] European Free Trade Association, 'General Data Protection Regulation incorporated into the EEA Agreement' (*European Free Trade Association*, 6 July 2018) <https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291> accessed 15 August 2023; European Commission, 'Data Protection in the EU' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> accessed 15 August 2023.
[59] European Free Trade Association, 'General Data Protection Regulation incorporated into the EEA Agreement' (n 58); European Commission, 'Data Protection in the EU' (n 58); European Free Trade Association, 'Data Protection' (*European Free Trade Association*) <https://www.efta.int/EEA/Data-Protection-505036> accessed 15 August 2023
[60] GDPR; European Data Protection Supervisor, 'The History of the General Data Protection Regulation' (n 17).
[61] Oskar Josef Gstrein and Andrej Janko Zwitter, 'Extraterritorial application of the GDPR: promoting European values or power?' (2021) 10(3) Internet Policy Review 1, <https://doi.org/10.14763/2021.3.1576> accessed 14 June 2023.
[62] Islam and Karim (n 9) 534.

due to its 'overarching provisions, exclusive market power and extensive extraterritorial scope'.[63] This paper will subsequently explore the extraterritorial scope of the GDPR as it greatly impact businesses of various sales and services in third countries such as Malaysia.[64]

2.2 Scope of Application of the GDPR

The GDPR encompasses a broad coverage on any processing of personal data, whether processed using automated means and which forms or intends to form part of a filing system.[65] As opposed to the PDPA, the GDPR does not confine its application purely to commercial transactions given that it recognises public authorities and agencies as controller and/or processor.[66] It is also observed that the GDPR defines personal data broadly as 'any information relating to an identified or identifiable natural person' which includes name, location data and online identifier.[67] Akin to the PDPA, the processing of personal data by natural persons which relates to a purely personal or household activity are exempted from the GDPR.[68] Additionally, the GDPR is not applicable if the processing activity falls outside of the EU law, or carried out by competent public authorities for detection or prevention of crimes and public security matters, which are covered under the Law Enforcement Directive[69].[70]

Article 3 of the GDPR stipulates the extraterritoriality effect of the GDPR, which is far-reaching. It applies if the controller and/or processor has any establishment in the EU;[71] the processing or monitoring activities involve individuals in the EU;[72] or the GDPR applies pursuant to public international law[73].[74] Given the self-explanatory of the last condition, the author will elaborate further on the first two situation.

---

[63] Islam and Karim (n 9) 534.
[64] Yakovleva and Irion, (n 10) 201.
[65] GDPR, art 2(1).
[66] GDPR, art 4(7); GDPR, art 4(8).
[67] GDPR, art 4(1).
[68] GDPR, art 2(2)(c).
[69] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2008] OJ L 119/89 ("**LED**").
[70] GDPR, art 2(2)(a); GDPR, art 2(2)(d).
[71] GDPR, art 3(1).
[72] GDPR, art 3(2)(a).
[73] GDPR, art 3(2)(b).
[74] GDPR, art 3; European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' (*European Data Protection Board*, 7 January 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_0.pdf> accessed 15 August 2023.

Firstly, it applies to processing of personal data of an establishment of a controller and/or processor within the EU and this irrespective of whether the processing takes place in the EU.[75] The European Data Protection Board ("**EDPB"**) views that this criteria applies to controller and processor, however, the criteria of establishment must be ascertained separately.[76] The mere contractual relationship between the controller and/or processor does not automatically trigger the application of this provision on both controller and processor in event one of them is established outside the EU.[77] Where the controller based in the EU chooses to engage a non-EU processor, there is an indirect obligation conferred on the non-EU processor in addition to the CBPDT restrictions prescribed in the GDPR.[78]

Secondly, the GDPR extends its arm to cover any establishment of controller and/or processor outside the EU region under two limbs.[79] The first limb is where the processing of personal data relates to the offering of goods and/or services to individuals in the EU.[80] The second limb is the involvement of monitoring of individuals in the EU which takes place within the EU.[81] It is crucial to note that the protection of individuals would cover any persons in the EU, regardless of their nationality or place of domicile.[82] It is helpful to consider that the GDPR only applies to processing of activities which are 'intentionally' targeted at individuals in the EU and does not include incidental or inadvertent situations. Further, the assessment of whether the GDPR is relevant is at the time the goods or services were offered and the duration of the offer is immaterial for consideration on whether the GDPR applies.[83] There must be an element of 'targeting' the individuals in the EU in offering goods/services or to carry out monitoring activities in addition to the processing activities requirement for the GDPR to apply.[84] The mere processing of personal data of individuals in the EU does not suffice to trigger the application of the extraterritoriality effect.[85] In respect of the monitoring of behaviour of a data subject in the EU, the monitoring activities must take place in the EU.[86] It may be considered as a

[75] GDPR, art 3(1).
[76] European Data Protection Board, 'Guidelines 3/2018' (n 74) 10.
[77] ibid.
[78] GDPR, art 28; GDPR, Chapter V; European Data Protection Board, 'Guidelines 3/2018' (n 74) 11.
[79] GDPR, art 3(2).
[80] GDPR, art 3(2)(a).
[81] GDPR, art 3(2)(b).
[82] GDPR, recital 14.
[83] European Data Protection Board, 'Guidelines 3/2018' (n 74) 15.
[84] ibid.
[85] ibid.
[86] GDPR, art 3(2)(b); European Data Protection Board, 'Guidelines 3/2018' (n 74) 19.

behavioural monitoring activity if it is to track individuals on the internet or through other means of technology to predict personal preferences and interests such as smart devices.[87] To name a few: monitoring activities include use of cookies on the internet, CCTV, market surveys and geo-localisations activities.[88]

2.3 Current Judicial Position of Data Protection in EU

The EC issued its first report in June 2020, two years after the commencement of operation of the GDPR in 2018 as required, after an evaluation was conducted to assess its application and functioning of Chapter V on CBPDT avenues and Chapter VII on cooperation and consistency application between independent supervisory mechanisms.[89] Chapter VII only applies to controller and/or processor with an EU establishment.[90] The next report is anticipated to be four years after June 2020.[91] The issued report suggests that the GDPR has effectively met its objectives to promote and increase awareness to individuals of their PDP, besides to ensure secure free movement of personal data within the EU.[92] With more individuals being apprised of their legal entitlements and the legal recourse they can resort to, the report finds a need to facilitate the exercise of such rights through a harmonised and effective enforcement mechanism which is linked to enhance the cooperation and consistency mechanisms across EU.[93] Actions have set in motion through a recent proposal by the EC to necessitate improvements in a multitude of areas such as complaint process and procedural rights and dispute resolution.[94] Examining the scope of this proposal is beyond the scope of the paper, however, it is presently at the feedback stage until September 2023 and the author observes this as a prudent initiative to enhance the GDPR and as an exemplar of PDP framework.[95] The author will delve into the approaches taken by the PDPA and the GDPR on CBPDT.

---

[87] GDPR, recital 24; European Data Protection Board, 'Guidelines 3/2018' (n 74) 19.
[88] ibid, 20.
[89] GDPR, art 97(1); GDPR, art 97(2).
[90] European Data Protection Board, 'Guidelines 3/2018' (n 74) 13.
[91] GDPR, art 97(1).
[92] European Commission, 'Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM (2020) 264 final, 4.
[93] ibid, 8.
[94] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council' COM (2023) 348 final.
[95] European Commission, 'Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation' (*European Commission*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en> accessed 15 August 2023.

[D] CHAPTER 3: OVERVIEW OF CROSS-BORDER PERSONAL DATA TRANSFER IN MALAYSIA VS THE EUROPEAN UNION

3.1 Position of the PDPA

Section 129 of the PDPA is the governing provision on CBPDT. It imposes a general prohibition on personal data transfer outside Malaysia, however, this restriction is not absolute per se, as there are means prescribed under the PDPA permitting such transfer.[96] One of the situations that allows CBPDT is where the PDPA-Ministry had considered the recommendations of the PDPA-Commissioner and approved a specific third country for free movement of personal data.[97] The discretion is contingent upon the evaluation of third country on whether there is 'substantially similar' protection as per the PDPA or if there are 'adequate level of protection' with regards to the processing of personal data.[98] This has a similar application as the adequacy mechanism under the GDPR.[99] Ever since its enactment, the PDPA maintained the whitelist approach and in 2017, the PDPA-Commissioner issued a draft Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017 ("**PDPA Whitelist Order**") proposing a list of jurisdictions which have been whitelist, for example, the EEA, the UK and Switzerland.[100] The draft PDPA Whitelist Order was not passed and it remains status quo with no jurisdictions being whitelisted.[101]

In 2020, the PDPA-Ministry issued a public consultation with a proposed revision to completely reverse the whitelist approach to blacklist for CBPDT.[102] This succinctly means that Malaysia recognises all third countries as having complied with its requirement, i.e. having substantially similar or adequate level of protection, unless there are recommendations to blacklist a jurisdiction.[103] The PDPA permits CBPDT using another means, by way of derogation which is premised on explicit consent obtained beforehand or there is necessity to

---

[96] PDPA, section 129(1).
[97] ibid.
[98] PDPA, section 129(2).
[99] GDPR, art 45.
[100] Hogan Lovells Publications, 'Malaysia Publishes draft "White List" for personal data exports' (*Hogan Lovells*, 27 April 2017) <https://www.hoganlovells.com/en/publications/malaysia-publishes-draft-white-list-for-personal-data-exports> accessed 15 August 2023.
[101] Baker McKenzie, 'International Data Transfer' (*Baker McKenzie*, 30 December 2022) <https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/malaysia/topics/international-data-transfer> accessed 15 August 2023.
[102] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18).
[103] Herbert Smith Freehills, 'Privacy law reform in Malaysia: One step closer to mandatory breach notification' (*Herbert Smith Freehills*, 17 August 2022) <https://hsfnotes.com/data/2022/08/17/privacy-law-reform-in-malaysia-one-step-closer-to-mandatory-breach-notification/> accessed 15 August 2023.

transfer personal data outside Malaysia.[104] The author will discuss the workings of derogation as a mechanism of CBPDT in ***Chapter 6***.

3.2 Position of the GDPR

Like the PDPA in its restriction on CBPDT, the GDPR enforces a non-absolute prohibition unless a processing activity falls within the ambit of exceptional circumstances accorded by the GDPR.[105] It is paramount to note that prior to any CBPDT, each of the individual processing task must comply with the PDP provisions enumerated in Articles 5 and 6 of the GDPR.[106] The EDPB clarified that Chapter V of the GDPR applies when there is CBPDT, subject to the fulfilment of three conditions which are: firstly, the controller and/or processor is subject to the GDPR for processing of personal data; secondly, personal data is disclosed and processed via transmission by either a controller and/or processor to another controller and/or processor, whether done independently or jointly; and lastly, the recipient of the personal data is located in a third country and this is regardless of whether the recipient is subject to the extraterritorial effect of the GDPR.[107] The advanced obligation is imposed on controller and/or processor to ensure compliance with the GDPR especially when such personal data transfer involves third countries or international organisations, including any onward personal data transfer.[108] Even if a processing task took place outside the EU/EEA, Chapter V of the GDPR is not applicable in absence of data transmission.[109]

Generally, there are three avenues legally permitting CBPDT outside EU/EEA.[110] Firstly, a third country may benefit from the adequacy mechanism which falls within the purview of the EC.[111] Secondly, the utilisation of appropriate safeguards as CBPDT tools by controller and/or processor.[112] Thirdly, the application of derogations in exceptional circumstances.[113] Christopher Kuner regards that derogation do not in itself constitutes a layer of security for

[104] PDPA, section 129(3).
[105] GDPR, art 44.
[106] ibid.
[107] European Data Protection Board, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR' (*European Data Protection Board*, 14 February 2023) 3 <https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf> accessed 15 August 2023.
[108] GDPR, art 44.
[109] European Data Protection Board, 'Guidelines 05/2021 on the Interplay' (n 107) 8.
[110] GDPR, chapter V.
[111] GDPR, art 45.
[112] GDPR, art 46.
[113] GDPR, art 49.

PDT, but rather it acts as a fall-back mechanism in default of an adequacy and appropriate safeguard mechanism.[114]

Fundamentally, the necessity to safeguard the PDP rights of natural persons remains consistent regardless of the avenues of CBPDT be it adequacy or appropriate safeguard, however a point to note is the level of protection that is maintained varies depending on the legal basis for PDT.[115] Adequacy mechanism is primarily concerned with the extent of protection conferred by the third country and if it is essentially equivalent to the EU framework.[116] The EC evaluates a diverse aspects of the legal framework of the third country, which will be discussed extensively in ***Chapter 4***.[117] The requirement to procure specific approval from the EC on CBPDT may be dispensed with once an adequacy decision is adopted.[118] Conversely, the appropriate safeguard is a pre-authorised set of devices by supervisory authorities to aid in CBPDT.[119] This is a means of resort when there is a lack of adequate legal system in the third country.[120] The author will elaborate on the various avenues of CBPDT below.

3.2.1 Interrelation between Extraterritoriality Reach in Article 3 of the GDPR vs Data Transfers Prohibitions in Chapter V of the GDPR

The author finds it pertinent to discuss the interplay between the extraterritoriality nature of the GDPR and the CBPDT prohibitions. The EDPB suggests that Chapter V of the GDPR is primarily intended to supplement the territorial scope of the GDPR and to mitigate any possible risks arising from Article 3 of the GDPR.[121] In situations where CBPDT are implicated, it is inevitable that such processing may be subjected to governing laws of third countries which personal data importers are mandated to uphold.[122] There may be risks arising from the implementation of third countries' laws which could exceed the 'necessary and proportionate' test and compromise the commitment pledged by EU in its attempt to heighten the personal

[114] Christopher Kuner, 'Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection' (2021) University of Cambridge Faculty of Law Research Paper No. 20/2021, 15 <https://ssrn.com/abstract=3827850> accessed 15 August 2023.
[115] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (GC, 16 July 2020), Opinion of AG Saugmandsgaard Øe ("**Schrems II AG Opinion**), para 117.
[116] Schrems II AG Opinion, para 119; Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (GC, 16 July 2020) ("**Schrems II**"), para 105.
[117] GDPR, Article 45(2).
[118] Schrems II AG Opinion, para 119.
[119] ibid, para 120.
[120] ibid.
[121] GDPR, chapter V; European Data Protection Board, 'Guidelines 05/2021 on the Interplay' (n 107) 6.
[122] ibid.

data protection rights of individuals.[123] Christopher Kuner, in drawing comparison between Article 3 and Chapter V of the GDPR, expressed that these rules are designed to deal with two separate situations, however he notes that ultimately, they aim to safeguard against entities outside the EU/EEA, whether through direct contact with individuals in the EU/EEA or through PDT through an EU establishment.[124]

3.2.2 Schrems Case Series

The author finds its useful to outline the case of Schrems I[125] (along with its sequel, Schrems II[126]) which are the landmark cases pertaining to CBPDT particularly on adequacy and appropriate safeguards. Briefly, the cases escalated to the CJEU for its assessment on the validity of the adequacy decision adopted by the EC in favour of the United States ("**US**") for CBPDT outside EU/EEA to the US known as the Safe Harbour and Privacy Shield.[127]

The CJEU in Schrems I held that whilst the term 'adequacy' prescribed in the Directive is lenient in that the laws of third countries are not expected to be identical or moulded based on the EU framework, there should be an adequate level of assurance portrayed by the third country which should be high standing and essentially equivalent to the GDPR.[128] The test of essentially equivalent is based on assessment of domestic laws and international commitments of third country, amongst other things, with a recognition of the personal data protection right under the Charter.[129] Additionally, the CJEU reinforced the position that the effective level of protection shall be assured and maintained throughout the PDT process whether within or outside the EU/EEA.[130]

The case of Schrems I is where Safe Harbour decision was struck out and this brought the Schrems II case into the picture. Schrems II concern the validity of revised adequacy decision of the EC known as the Privacy Shield as well as the Standard Contractual Clauses ("**SCC**") utilised for the CBPDT.[131] In consideration of the case, the CJEU held the invalidity of the Privacy Shield, however went on to decide that the SCC used for CBPDT between the trading

[123] European Data Protection Board, 'Guidelines 05/2021 on the Interplay' (n 107) 6.
[124] Kuner (n 114) 30-31.
[125] Case C-362/14 Maximillian Schrems v Data Protection Commissioner (GC, 6 October 2015] ("**Schrems I**").
[126] Schrems II.
[127] Schrems I; Schrems II.
[128] Schrems I, para 73.
[129] CFR, art 8; Schrems I, para 71.
[130] Schrems I, para 72.
[131] Schrems II, para 68.

partners as a valid transfer tool and legitimise the CBPDT.[132] The operation of adequacy and appropriate safeguards appear to be different, however, the CJEU viewed them as two interrelated principles and with that imported the element of 'essential equivalence' from adequacy decision mechanism to the SCC.[133] It is to ascertain whether the use of the SCC in Schrems II accords sufficient protection with supplementary measures in place.[134] The 'essentially equivalent' criteria was intended to uphold the personal data protection right by narrowing the gap between the third country legal systems to the GDPR and Maria Tzanou viewed this upgrade of PDP to fundamental right should be regarded as executing the mandatory 'EU institutions' fundamental rights protective duty'.[135] This paper will expound further on the findings of the CJEU in Schrems II and its impact to the practicality of CBPDT in subsequent chapters. At this juncture, the author considers it timely to state that the EU-US have adopted a new adequacy decision: the EU-US Data Privacy Framework ("**EU-US DPF**") on the 10th of July 2023 to advance international ties given the invalidity of earlier adequacy decisions, which will be explored in ***Chapter 4.2***.[136]

[132] Schrems II, para 149; Schrems II, para 201.
[133] Schrems II, paras 134 – 135; Róisín Áine Costello, 'Schrems II: Everything Is Illuminated?' (2020) 5 European Papers 703, 1053 <https://www.europeanpapers.eu/sites/default/files/EP_eJ_2020_2.pdf> accessed 15 August 2023.
[134] Schrems II, paras 134 – 135; Costello (n 133) 1053.
[135] Maria Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Bloomsbury 2021) ch 7.
[136] European Commission, 'Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework' C(2023) 4745 final <https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf> accessed 15 August 2023 ("**EU-US DPF**"); European Commission, 'Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows' (*European Commission*, 10 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721> accessed 15 August 2023.

[E] CHAPTER 4: ADEQUACY DECISION MECHANISM

4.1 Overview of Adequacy Decision

One of the avenues permitting CBPDT between two countries is adequacy decision, whereby the decision-making is done at the international level.[137] The evaluation of 'adequate level of protection' is a mutual attribute reflected in the PDPA as well as the GDPR.[138] As discussed earlier, although the PDPA provides such an avenue for CBPDT, there is no enactment of the PDPA Whitelist Order as it was at the public consultation phase, thus retained its status quo to date.[139]

The EC, on the other hand, exercised its powers under the GDPR in its issuance of adequacy decision to third countries or international organisations.[140] The adequacy decision is an implementing act of the EC intended to create coherence in the implementation of the GDPR.[141] This is evident through the recognition of the data protection legislation of up to 15 jurisdictions[142] such as Israel, Japan and Canada as having adequate data protection as the GDPR.[143] The GDPR is seen as the 'global standard-setter' in the aspect of the digital trading and where an adequacy decision is adopted in favour of a third country, this serves as an attractive feature to promote trade.[144]

There is a four-tiered process in the adoption of the adequacy decision, which begins with a proposal put forth by the EC ("**Adequacy Decision Proposal**").[145] Subsequently, this

---

[137] GDPR, art 45.
[138] PDPA, section 129(1).
[139] Christopher & Lee Ong, 'Personal Data Protection Updates – Public Consultation Paper No. 1/2017 – Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017' (*Rajah & Tann Asia*, April 2017) <https://www.christopherleeong.com/media/2785/personal-data-protection-transfer-of-personal-data-to-places-outside-malaysia-order-2017.pdf> accessed 15August 2023.
[140] GDPR, art 45.
[141] GDPR, art 45(2); GDPR, art 93(2); European Union, 'Implementing Acts' (*EUR-Lex*) <https://eur-lex.europa.eu/EN/legal-content/glossary/implementing-acts.html#:~:text=These%20acts%20aim%20to%20create,have%20individual%20or%20general%20applications.> accessed 15 August 2023; Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141).
[142] At the time of writing in August 2023, the European Commission recognised 15 jurisdictions as follows: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States, and Uruguay.
[143] European Commission, 'Adequacy Decisions' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 15 August 2023.
[144] European Commission, 'Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' (n 92) 3 - 11.
[145] European Commission, 'Adequacy Decisions' (n 143); Data Protection Commissioner, 'Transfers of Personal Data to Third Countries or International Organisations' (*Data Protection Commissioner*) <https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations> accessed 15 August 2023.

Adequacy Decision Proposal will be circulated to the EDPB for its opinion.[146] The third tier of the process is to allow the representatives of various EU member states to deliberate on the Adequacy Decision Proposal and when their approval has been obtained, the final tier of the process would be the adoption of the adequacy decision by the EC.[147] It is imperative to note that in the midst of the process for adoption of adequacy decision, the EC may be required to carry out audit functions prior to the certification and issuance of adequacy decision.[148] The involvement of many different entities for the adoption of the adequacy decision may be a long process which may take up to years, for instance, the initiatives to explore adequacy mechanisms by the EU with Japan and Korea in 2017, which however took approximately four years for adoption of the adequacy decision.[149] This may be further prolonged due to the completion of auditing process prior to certification and issuance of adequacy decision in favour of the third country.[150] As Alex Voss pointed out, the lengthy process of adequacy assessment may constitute a hindrance to third countries from being interested to consider this route for benefit of CBPDT.[151]

From the EU/EEA perspective, it is however not surprising that the entire process is prolonged as there is a high level of requirement to be achieved given that the data protection is recognised as a fundamental rights pursuant to the Charter which should neither be compromised or undermined under any circumstances.[152] After all, there is a multitude of facets of the third country in question to be considered by the EC in assessing the level of data protection accorded before putting forward the proposal for adequacy mechanisms, namely the laws and regulations, existence and effective functioning of the independent supervisory authority and international commitment.[153] In respect of international commitments, this may be demonstrated through legally binding conventions or instruments entered into by the third

[146] European Commission, 'Adequacy Decisions' (n 143); Data Protection Commissioner, 'Transfers of Personal Data to Third Countries or International Organisations' (n 145).
[147] ibid.
[148] Elisabeth Meddin, 'The Cost Of Ensuring Privacy: How The General Data Protection Regulation Acts as a Barrier To Trade In Violation Of Articles XVI And XVII Of The General Agreement On Trade In Services' (2020) 35(4) American University International Law Review 997, 1017.
[149] European Commission, 'Communication From The Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 final; Thomas Wahl, 'Commission Adopted Adequacy Decision for South Korea' (EUCRIM, 22 December 2021) <https://eucrim.eu/news/commission-adopted-adequacy-decision-for-south-korea/> accessed 15 August 2023.
[150] Elisabeth Meddin (n 148) 1017.
[151] Axel Voss, 'Position Paper on Fixing the GDPR: Towards Version 2.0' (*Axel Voss*, 25 May 2021) 30 <https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf> accessed 15 August 2023.
[152] Charter, art 8.
[153] GDPR, art 45(2).

country in question specifically in protection of personal data.[154] Greenleaf viewed that the rationale for this is to ensure there is a guarantee that the free flow permission of personal data shall not in any way exposes the EU citizens or data subjects protected under GDPR to risk of data breach.[155]

To ensure coherence and uniformity within the EU/EEA, the EC may, where it deemed appropriate and necessary, issue a decision in favour of a third country or international organisation and such decision has the effect of allowing free flow of personal data from the EU/EEA without any subsequent authorisation, safeguards, or measures in place.[156] A legally enforceable adequacy decision adopted by the EC may be one which is applicable either across the jurisdiction as a whole, territory, sectoral or within an international organisation.[157] The binding legal effect of adequacy decision is to assimilate the CBPDT as part of the 'intra-EU transmissions of data', however they are not perpetual as regular reviews of every four years will be carried out by the EC to ensure that the high standard is maintained or further enhanced to align with the Charter,[158] failing which the adequacy decision may be revoked.[159] The EC bears the legal responsibility of overseeing the development of the legislation in the third country in question which may impact the issued or adopted adequacy decision.[160] In any event where the adequacy decision may be affected by the development of the laws and regulations in the third country in a way that jeopardizes the fundamental right, the EC may repeal, amend or suspend the decision provided opinion of the EDPB has been obtained beforehand and prior consultation with the third country is carried out before deciding on a suitable course of action.[161] The validity of an adequacy decision may also be challenged and be subjected to an examination by the CJEU where a complaint is lodged to the national supervisory authority to challenge its validity and an example would be the Schrems case series.[162]

[154] GDPR, art 45(2)(c).
[155] Greenleaf, 'Free Trade Agreements' (n 16) 181-212.
[156] GDPR, recital 10; GDPR, recital 103; European Commission, 'Adequacy Decisions' (n 143).
[157] GDPR, art 45(1); Laura Drechsler, 'What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights' (2019) Jusletter IT <https://ssrn.com/abstract=3549252> accessed 15 August 2023.
[158] GDPR, art 45(3).
[159] GDPR, recital 103; GDPR, recital 107; Schrems II, para 118; European Commission, 'Adequacy Decisions' (n 143).
[160] GDPR, art 45(2).
[161] GDPR, art 45(5); GDPR, art 45(6); GDPR, art 70(1)(s).
[162] Schrems II, para 119.

The complexity of the assessment of adequacy decision is deciphering the threshold of 'adequacy' protection. In comparison to the PDPA which is silent on the evaluation criteria, the GDPR shed some light on the diverse aspects of third country jurisdiction which would aid the EC in determining whether the third country or international organisation shares the same level of adequacy as the GDPR.[163] Some additional key elements worth noting include the human rights protection accorded to individuals and access of personal data to governmental bodies,.[164] These elements prescribed in the GDPR suggest that the EU policymakers place utmost emphasis on the strength and extensiveness of data protection frameworks as indicators of commitment, assurances and adherence to data protection rights at an equivalent level as the EU.[165]

Article 29 Working Party ("**A29WP**"), the predecessor of the EDPB expounded on the deciding factors for adequacy and viewed that the mere existence of laws and regulations prescribing legal entitlement of data subjects and identifying the responsibilities of controller and/or processor as being insufficient if there is an absence of enforceability of the governing provisions in practice.[166] Enforcement mechanisms are highly crucial to implement and ensure adherence of the intended effect of EU legislators.[167] The quintessence of the adequate protection by virtue of Article 45 of the GDPR is the presence of two components to ensure a 'meaningful analysis' is carried out which are the coverage and the means for implementation for an effective data protection.[168]

4.2 Newly Adopted EU-US Data Privacy Framework

The invalidity of the Safe Harbour[169] and Privacy Shield[170] resulted from the Schrems case series served as valuable lessons for the EU-US to introduce EU-compliant data protection obligations as framework for businesses and international organisations which align with the

[163] GDPR, art 45(2).
[164] ibid.
[165] ibid.
[166] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141) ch 1.
[167] ibid.
[168] ibid.
[169] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce OJ L 215/7 ("**Safe Harbour**").
[170] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield OJ L 207/1 ("**Privacy Shield**").

principles of GDPR on CBPDT, case precedents and the EU laws and regulations. Their concerted efforts materialised with the EC adopted a new adequacy decision on the 10th of July 2023.[171] The EC is satisfied with the legal framework of the USA, which includes two new implementations of the 'Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' ("**US Executive Order**") and the Data Protection Review Court issued by the U.S. Attorney General' ("**US Review Court**") to address the deficiencies of the US law as pointed out by the CJEU in Schrems II.[172] Briefly, the US Executive Order specifies the legally binding safeguards and draws the limitation in respect of processing activities pertaining to signal intelligence and national security purposes,[173] however, these safeguards shall also be subject to the basic PDP principles of the GDPR.[174] Additionally, the US Review Court is a redress mechanism newly set up to handle and resolve complaints arising from data subjects pertaining to purported violations of US law governing signal intelligence activities.[175]

The effect of the EU-US DPF allows free flow of PDT between controller and/or processor in the EU to the US, with no further authorisation required, provided that the recipient is eligible as a certified organisation under the EU-US DPF.[176] To effectuate CBPDT between EU-US, the operation of this initiative is done voluntarily by interested organisations.[177] Recertification on an annual basis would be necessary to ensure eligibility.[178] The accountability principles portrayed in GDPR similarly applies to US processors who are required to adhere to the EU controllers and, where sub-processors are involved, the same obligations extend to them as well through a contractual document between the US processors.[179] The author observes that the basic data principles enshrined in the GDPR and the guiding principles introduced by the EDPB or A29WP is preserved,[180] if not reinforced, and the author opines that this will be relevant and advantageous to this paper in the assessment of Malaysia to achieve adequacy based on its political, judicial and legal landscape.

[171] EU-US DPF (n 136) 3.
[172] Schrems II, paras 178 – 201; EU-US DPF (n 136) 3.
[173] EU-US DPF (n 136) ch 3.2.1.2.
[174] EU-US DPF (n 136) recital 160.
[175] EU-US DPF (n 136) ch 3.2.3
[176] EU-US DPF (n 136) 3.
[177] ibid.
[178] EU-US DPF (n 136) 4.
[179] ibid.
[180] EU-US DPF (n 136) ch 2.2.

4.3 Guiding Principle for EU-Malaysia

The EC acknowledged that where two countries are more aligned in their PDP system, it would eventually lead to an increase and smoother international flows of PDT which appeals to interested third countries to improve trade through conformity with the GDPR.[181] However, Elisabeth Meddin opined that the adequacy decision is a system which is both 'flawed and arbitrary' and consequentially this acts as a hindrance to trade for non-EU businesses to penetrate the EU market.[182] The inconsistencies in the evaluation of adequacy of third countries despite the significant influence of the GDPR to third countries to the extent of aligning or revamping their legislation to be GDPR-like raised doubts and may shun third countries away.[183]

At the time of writing this paper, Malaysia has yet to be part of the 15 jurisdictions to have an adequacy decision in place, hence the mandatory requirement applies for personal data transmitted from EU to Malaysia to be subjected to additional PDP safeguards.[184] In this paper, the author intends to review and explore whether the PDPA would qualify Malaysia as having adequate protection equivalent to the GDPR in the CBPDT allowing adequacy decision to be adopted by the EC. The primary objective of the test of 'essentially equivalent' is to establish the essence of the requirements in data protection legislation of the third country and not to mirror each of the provisions in the GDPR.[185] Of assistance is the guide prepared by the A29WP to enlighten third countries or international organisations such as Malaysia which may be desirous in obtaining adequacy.[186] To summarise the guidance note prepared by the A29WP, the salient precondition expected entails two main body of principles, namely: (i) the central concepts and elements of data protection for both general and specific processing; and (ii) procedural and enforcement mechanisms.[187]

In doing so, the author finds it beneficial to examine the PDPA in terms of its scope of application, the cardinal principles of data protection enshrined in the PDPA, legal rights and remedies accorded to the data subjects as well as the enforcement mechanisms. Simultaneously,

[181] European Commission, Communication From The Commission To The European Parliament And The Council: Exchanging and Protecting Personal Data in a Globalised World COM (2017) 7 final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN> accessed 15 August 2023.
[182] Elisabeth Meddin (n 148) 1015.
[183] Axel Voss (n 151) 30; Islam and Karim (n 9) 534.
[184] European Commission, 'Adequacy Decisions' (n 143).
[185] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141).
[186] ibid.
[187] ibid.

the author will also conduct a review of the GDPR in the same vein for comparative analysis on the suitability of Malaysia in adopting an adequacy decision.

4.4 Cardinal Principles of Data Protection

To begin with, the PDPA has seven PDP principles encapsulated in Section 5(1) of the PDPA namely: the general principles; notice and choice principle; disclosure principle; security principle; retention principle; data integrity principle; and access principle.[188] Similarly, there are seven essential principles under GDPR prescribed in Article 5 of the GDPR, which are: lawfulness, fairness and transparency principle; purpose limitation; data minimisation; accuracy principle; storage limitation; integrity and confidentiality; and accountability.[189] This paper will discuss the different principles below and evaluate resemblance or differences between the PDPA and GDPR.

4.4.1 Legal bases for Legitimate Processing

Personal data can be broadly distinguished by the general personal data and sensitive personal data. The general personal data are information pertaining to any commercial transactions, while the sensitive personal data refers to personal information relating to the physical or mental condition of a data subject and extends to the religious beliefs and political opinions of data subject.[190] The processing of personal data are legal if the processing is premised on the consent of data subjects,[191] or where the processing is necessary.[192] Whilst consent is a legal basis applicable to processing of personal data of all kinds, there is a higher threshold imposed on sensitive personal data, whereby explicit consent is required before processing.[193] Processing of personal data premised on necessity is permitted on the basis of entering or completing a contractual obligation; adherence to legal requirements; safeguard the vital interests of data subject; pursuit of interest of justice; or to exercise functions in line with applicable laws.[194] Additionally for sensitive personal data, processing is necessary if it falls within the context of healthcare purposes.[195] It is crucial that the legitimate basis for processing

[188] PDPA, section 6(1).
[189] GDPR, art 5.
[190] PDPA, section 4.
[191] PDPA, section 6(1).
[192] PDPA, section 6(2).
[193] PDPA, section 6(1)(b); PDPA, section 40.
[194] PDPA, section 6(2).
[195] PDPA, section 40(1)(b)(iv).

directly relates to the activity of data user, it must be necessary to do so and the personal data involved is adequate but not excessive in relation to that purpose.[196]

There are six legal bases recognised by the GDPR for valid processing of personal data stipulated in Article 6 of the GDPR.[197] A broad comparison reveals that the PDPA and the GDPR share similar features in this aspect. The controller and/or processor may legally process the personal data if consent has been obtained, or where it is necessary to do so, to meet contractual and legal obligations, vital interest of individuals, public and legitimate interest and processing permissible under the GDPR.[198] These bases are not restricted as the GDPR welcomes additional or clearer provisions for processing in context or legal obligation and public interest.[199]

The explicit consent of data subject is necessary to legitimise the processing of sensitive personal data under the GDPR.[200] There are additional grounds for processing of sensitive personal data, i.e. in the context of preventive or occupational medicine,[201] public health,[202] and in research or scientific purposes.[203] The GDPR requires the controller to carry out an assessment of factors prior to further processing if the personal data are processed on legal bases other than consent of data subject or if it is pursuant to the necessity and proportionality principle, also known as the compatibility test.[204] The criteria includes linkage of initial and further processing of personal data, the context and nature of personal data collected, as well as the possible ramification to further process and appropriate safeguards established.[205]

4.4.2 Transparency

The notice and choice principle under the PDPA has the same bearing as the transparency principle under the GDPR. The PDPA prescribes the data user to promptly notify the data subject, by way of a written notice, of the intended processing activities to be carried out by

[196] PDPA, section 6(3).
[197] GDPR, art 6.
[198] GDPR, art 6(1).
[199] GDPR, art 6(2).
[200] GDPR, art 9(2)(a).
[201] GDPR, art 9(2)(h).
[202] GDPR, art 9(2)(i).
[203] GDPR, art 9(2)(j).
[204] GDPR, art 6(4).
[205] ibid.

them.[206] The underlying rationale is to apprise the data subject of the information relating to the processing activities which includes the specific details of the personal data to be processed, the purpose of processing, the rights granted to the data subject, recipients to whom it may be shared to, the choices and means available to data subject, whether the supply of personal data is mandatory or voluntary and whether any possible consequences for failing to provide such personal data.[207] The data user shall notify the data subject 'as soon as practicable' at a time when data subject is first asked to supply information or when personal data is first collected for use.[208] Similarly, such notice must be given before further processing is made for purposes other than the intended purpose for which personal data is collected or prior to disclosure to third party.[209] The general PDPA-COP elucidates that communication may be done through numerous methods, by way of email, post, text message or display of messages at kiosks systems.[210]

The transparency principles under the GDPR is promulgated with the primary intention to ensure data subject is informed or communicated by controller and/or processor on details of the processing activities directly collected from data subject.[211] The conveyance of the information to the data subject must be done in a clear, plain language, concise, intelligible, and easily accessible manner to aid the data subject to understand the information before making any decision regarding their personal data.[212] Contrary to the PDPA, the GDPR mandates the controller who has indirectly obtained the personal data of an individual through a third party to also specify the source where the personal data originate from and whether these existing personal data were publicly available.[213] Indicating the source of personal data is an additional information that data controller has to notify data subject, in addition to other information stated in Article 14(1)(a) GDPR.[214] Any controller that intends to further process the personal data for reasons other than what was intended shall, prior to the processing of

[206] PDPA, section 7.
[207] ibid; Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 13-14.
[208] PDPA, section 7(2).
[209] ibid.
[210] Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 15-16.
[211] GDPR, art 5(1)(a); GDPR, art 12; GDPR, art 13; GDPR, art 14.
[212] GDPR, art 12; GDPR, recital 39; Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (*Article 29 Data Protection Working Party*, 11 April 2018) WP260 rev 01 <https://ec.europa.eu/newsroom/article29/items/622227/en> accessed 15 August 2023.
[213] PDPA, art 14(2)(f).
[214] GDPR, art 14(1).

personal data, comply with the transparency principle by notifying data subject of the details of the further processing to ensure there is fair processing.[215]

4.4.3 Purpose Limitation

The PDPA generally restricts personal data processing activities unless: (i) there is lawful purpose directly related to the data user's commercial activities to process the personal data; (ii) such processing is necessary or directly related to the purpose; and (iii) the use of personal data for the intended purpose is not excessive.[216] Processing activities for purposes other than the initial purpose may be allowed under the PDPA subject to obtaining the data subject's consent, or where such processing is necessary pursuant to law, court order or public interest.[217] The data users shall record a list of disclosure to third parties for all the ongoing or completed processing activities.[218]

The GDPR contains similar right to disclosure as per the PDPA, which is an overlap of both the purpose limitation and the data minimisation principle. The purpose limitation principle permits collection of personal data which shall be strictly used for 'specified, explicit and legitimate purposes' and shall not be further processed in ways which contravenes the initial purpose for data collection.[219] Compatibility test shall be observed by the controller in determining whether there is a linkage between the initial and subsequent purpose as well as the nature of personal data.[220] Further processing of personal data under the GDPR is allowed in respect of archive purposes done in the 'public interest, scientific or historical research purposes or statistical purposes'.[221] However, they shall be subjected to appropriate technical and organisational measures to observe and be in line with the data minimisation principle.[222] The ground for processing must meet the test of adequacy, relevancy and limited to what is necessary for the intended purpose, and one of the practical solutions introduced is pseudonymisation.[223] In detail, pseudonymisation is a method introduced to enhance the data minimisation principle.[224] It is a process which disable personal data from attributing to a

[215] GDPR, art 13(3); GDPR, art 14(4).
[216] PDPA, section 6(3).
[217] PDPA, section 39; PDPA, section 8.
[218] PDPA, section 8(b); PDPA Regulations, reg 5.
[219] GDPR, art 5(1)(b).
[220] GDPR, art 6(4).
[221] GDPR, art 5(1)(b); GDPR, art 89.
[222] GDPR, art 89(1).
[223] GDPR, art 25(1).
[224] ibid.

specific data subject in absence of any use of additional information subject to having technical and organisation measures in place.[225]

4.4.4 Accuracy and Access

One of the principles encased in the PDPA is known as the data integrity principle.[226] In essence, it requires the data user to undertake appropriate actions to warrant that the personal data collected and processed by them are accurate, current, and not misleading, by virtue of the purpose for which it is collected.[227] The access principle enhance the data integrity principle as it allows the data subject to access the personal data and request corrective action of the personal data if the information is inaccurate, incomplete, misleading or outdate.[228] A data subject may avail itself of the right to correct personal data under the PDPA.[229] There is notable likeness in the data integrity principle adopted by the PDPA and the one reflected in the GDPR, under the accuracy principle.[230] Personal data collected shall be accurate and updated, if needed.[231] Where it is to the contrary, the GDPR mandates that reasonable undertakings be made after having considered the purpose for which the personal data is collected, to ensure that any inaccurate personal data be erased or rectified promptly.[232]

4.4.5 Security of Personal Data

The PDPA mandates the data users to accomplish action plans to assure the security of personal data.[233] Notably, the data users shall employ practical measures to ensure that the personal data collected are safeguarded from any unauthorised use or data loss.[234] The data users are directed to consider a wide array of factors prior to introducing effective methods to curb unwarranted data such as categories of personal information for processing, gravity of data loss, unauthorised or inadvertent disclosure of personal data, data repository of personal data.[235] Furthermore, the data user shall consider the implementation of security measures in the equipment installation, ways to secure and/or tighten the data transfers as well as to ensure that

[225] GDPR, art 4(5).
[226] PDPA, section 11; PDPA Regulations, reg 8.
[227] PDPA, section 11.
[228] PDPA, section 12.
[229] PDPA, section 34; PDPA, section 35.
[230] PDPA, section 12; GDPR, art 5(1)(d).
[231] GDPR, art 5(1)(d).
[232] ibid.
[233] PDPA, section 9.
[234] PDPA, section 9(1); PDPA, section 9(2).
[235] PDPA, section 9(1).

its authorised personnel are competent and trustworthy in the management of personal data.[236] Under the circumstances that data users delegate the processing activities to data processors, data users shall discharge its legal duty in making sure that the same level of commitment to protect personal data is demonstrated by the data processor in 'technical and organizational security measures' when processing data and shall take reasonable measures at all times in observing compliance.[237] There are practical measures set out in the Personal Data Protection Standard 2015 ("**PDPA Standards**") introduced in light of the PDPA Regulations which focused on setting out standards pertaining to security, retention and data integrity standards.[238] It is recommended that the contractual document between the data user and third party processor should consider implementation of a confidentiality agreement, restrictions on circumstances which warrant processing, security measures to be established and destruction or return of personal data under the control of the processor upon termination or expiry of the contractual obligations.[239]

Correspondingly, the GDPR appreciates the significance of security measures in place to secure the personal data collected.[240] It is mandatory for the controller and/or processor to guarantee that an appropriate level of security is observed using technical or organisational measures in the processing of personal data, and as preventive measures of any 'unauthorised or unlawful processing' and to preserve against any inadvertent data loss or destruction.[241] The commitment of the GDPR to assure security of personal data is evident through Article 32 of the GDPR which imposes responsibilities on the controller and/or processor to introduce appropriate security in place which corresponds to potential legal risks and consequences of data breach as well as the nature of personal data collected, through use of practical measures.[242] The use of pseudonymisation and encryption of personal data are introduced as mitigating efforts, in addition to the general prescription of ensuring the system security are effective by regular system check and assessment of the risks.[243] Moreover, the GDPR necessitates strict observation by controller and/or processor to ensure that its employees with access to personal

[236] PDPA, section 9(1).
[237] PDPA, section 9(2).
[238] Personal Data Protection Standards 2015 ("**PDPA Standards**"); The Personal Data Protection Commissioner Malaysia, 'Personal Data Protection Standards 2015' (*Personal Data Protection of Malaysia*) <https://www.pdp.gov.my/jpdpv2/assets/2019/09/BukuStandardPDP-2015.pdf> accessed 15 August 2023.
[239] Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 23.
[240] GDPR, art 5(1)(e).
[241] ibid.
[242] GDPR art 32(1).
[243] ibid; GDPR, recital 83.

data does not access such data in absence of instruction from the controller.[244] A controller and/or processor may exhibit their compliance using an approved code of conduct or certification mechanism, which this paper will explore in ***Chapters 5.3 and 5.4***.[245]

4.4.6 Retention of Personal Data

Aligned with the purpose limitation principle, the personal data shall not be kept for a period longer than what is necessary, hence the PDPA requires that the data user carry out viable solutions assuring that the personal data that are no longer necessary for its intended purpose be destroyed permanently.[246] The data user may consider pragmatic steps such as determination of retention period, maintain record of disposal of personal data, schedule a disposal timetable, prohibit use of computing cloud services or portable devices from unauthorized transfer of personal data.[247] In a similar trajectory, the GDPR forbids the storage of personal data beyond the necessary period required to achieve what is intended.[248] However, the GDPR acknowledges exceptions to this if it concerns public interest, archiving or research purposes.[249] Whilst longer retention period is allowed, it necessitates the establishment of appropriate technical and organisation measures to safeguard the personal data consistent with the data minimisation principle.[250]

4.4.7 Accountability

The accountability principle is an integral part of the data protection principles as it obligates the controller and/or processor to adhere to all the foundational data protection principles discussed earlier in ***Chapter 4.4***.[251] There is no specific provision in the PDPA although it does prescribe that the data users bear such legal obligations to comply with the data protection principles.[252] The author observes that only the security principle would confer obligations from the data user to the processor, however the onus to enter into an agreement and to prescribe the security measures appear to be in the hands of the data users.[253] It is imperative to note that the specific conferment of legal obligations on the data users are not extended to data

[244] GDPR, art 32(4).
[245] GDPR, art 32(3).
[246] PDPA, section 10.
[247] PDPA Standards, chapter 6 of Part II.
[248] PDPA, section 10; GDPR, art 5(1)(e).
[249] GDPR, art 89(1).
[250] GDPR, art 89.
[251] GDPR, art 5(2).
[252] PDPA, section 5(1).
[253] Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 23.

processors.[254] To emphasize, the PDPA specifically excludes data processors from the definition of 'data users'.[255] The notion to extend the 'accountability' obligations on the data processors is listed as a potential area of development.[256]

Under the GDPR, the roles of controller are indicative of the accountability principle.[257] Although the provision specifically states that the controller bears the responsibility to adhere to all the fundamental provisions, the author submits that the processor shall, to an extent applicable, be jointly responsible given that they are closely associated with one another whereby the processor takes strict instructions of the controller in respect of processing activities.[258] The GDPR obligates the controllers to ensure that its processors undertake to implement technical and operational measure in line with the GDPR to uphold the protection of data subjects.[259] Other responsibilities of the controller and processor entail the keeping of records of the processing activities, pursuit of data protection impact assessments, and effectuating data protection by design and by default.[260]

4.5 Rights Accorded to Data Subjects

Moving on, this paper seeks to explore the assortment of rights available to individuals in both jurisdictions, starting with the review of the PDPA followed by the GDPR. It is expected that the findings under this subchapter will assist the author in evaluating whether the PDPA had accorded adequate right to individuals for the safeguarding of their individual right as well as to meet the requirements for adequacy decision.

4.5.1 Access to Personal Data

The PDPA permits the data subject to request access to his/her personal data and related information from the data user including making copies of such personal data requested in an intelligible manner.[261] Besides, there is a deeming provision whereby the data access request by data subject similarly binds a data user who merely controls the processing of personal data without being in actual possession of the personal data in question.[262] Unless the data user has

[254] PDPA, section 5(1).
[255] PDPA, section 4.
[256] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18) 4.
[257] GDPR, chapter IV.
[258] GDPR, art 28(1); GDPR, art 28(3).
[259] GDPR, art 28(1).
[260] GDPR, art 30; GDPR, art 35; GDPR, art 25.
[261] PDPA, section 30(1); PDPA, section 30(2).
[262] PDPA, section 30(5).

provided a notice to data subject communicating the delay to meet the data access request,[263] or where there are justifiable reasons for which a data user may refuse access request of data subject,[264] it is a mandatory obligation on a data user to comply with such request within a stipulated time frame of twenty-one days.[265]

Conversely, the GDPR permits data subject to seek for a confirmation from the controller on whether there is processing of his/her personal data, and if so, the controller shall supply the specifics of the requested data and processing activities comprising of the register of recipients as well as providing a copy of the personal data.[266] If there is automated decision-making or profiling in the process, the data subject must be apprised of the logic involved behind such decision-making or profiling, the significance, and possible repercussions of such processing.[267] Any details of CBPDT shall also be informed to the data subject including presence of any appropriate safeguards in place.[268]

4.5.2 Rectification of Personal Data

Should the data subject under the PDPA becomes aware of any discrepancy, inaccuracies, misleading or any outdated personal data, be it through having sight of the copy of personal data or otherwise, the data subject may write to the data user to request for necessary data correction.[269] Provided that the data subject is satisfied that the data correction is necessary, such request should be attended by the data user within a specified period, or at a later date provided the delay has been communicated to the data subject.[270] Once the correction has been made, the data user shall furnish the data subject with the correct personal data and if disclosure were made to third parties prior to the disclosure, the data user shall notify the third party in writing along with the reasons for correction and a copy of the rectified information.[271] If the data user refuses to make correction, the same must be notified to the data subject providing reasons for refusal.[272] The right to rectification is a driving force of the data integrity principle with the primary aim of ensuring the personal data processed is accurate. This principle is

[263] PDPA, section 31(2).
[264] PDPA, section 32.
[265] PDPA, section 31(1).
[266] GDPR, art 15(1); GDPR, art 15(3).
[267] GDPR, art 15(1)(h).
[268] GDPR, art 15(2).
[269] PDPA, section 34(1).
[270] PDPA, section 35(1); PDPA, section 35(2).
[271] PDPA, section 35(1).
[272] PDPA, section 37.

similarly reflected in the GDPR. However, the position taken therein is straightforward whereby any requests for rectification of personal data must be done promptly without any delay.[273] The data subject may also complete his/her personal data through supplementary statement.[274]

4.5.3 Withdrawal of Consent

As this paper had explored, consent is a bedrock ground for legitimate data processing which symbolises individual's autonomy,[275] hence it is embedded in the PDPA that a data subject may similarly exercise its autonomy to withdraw his/her consent to the processing of personal data by a data user provided written notice is provided.[276] This is similarly recognised under the GDPR for withdrawal at any point in time.[277] The data user is compelled to cease all processing of personal data upon receipt of such notice from data subject.[278] Any failure to comply with the cessation of processing after receipt of the withdrawal notice exposes the data user to risk of legal ramifications upon conviction of an offence.[279] It is imperative to underscore that the failure of a data subject to enforce this right is not a waiver to other rights prescribed in PDPA.[280] The GDPR emphasised that the effect of such withdrawal only applies prospectively and not retrospectively.[281] This means that the legality of processing of personal data prior to the withdrawal of consent shall remain unaffected.[282]

4.5.4 Restrict Processing of Personal Data

The right to restrict processing of personal data is permissible under the PDPA and the GDPR, however applies in different context. A data subject under the PDPA may request the data user to cease processing or not begin with the processing if the data subject opined that it may cause unwarranted material damage or distress to any individual.[283] It is vital that such request be made within a reasonable time.[284] One cannot enforce such right if there is legitimate processing by way of any the legal bases mentioned in Section 6 of the PDPA to which personal

[273] GDPR, art 16.
[274] ibid.
[275] PDPA, section 6(1); PDPA, section 40(1)(a); GDPR, art 6(1)(a); GDPR, art 9(2)(a).
[276] PDPA, section 38(1).
[277] GDPR, art 7(3).
[278] PDPA, section 38(2).
[279] PDPA, section 38(4).
[280] PDPA, section 38(3).
[281] GDPR, art 7(3).
[282] ibid.
[283] PDPA, section 42(1).
[284] ibid.

data is processed.[285] Here, the data user has the option to decide on the request put forth by the data subject and shall convey their decision to the data subject in writing.[286] An unsatisfied data subject is entitled to escalate the refusal of data subject by filing a complaint to the PDPA Commissioner who may then consider such matter.[287]

As is available under the GDPR,[288] there must be either an intention by data subject to contest accuracy of his/her personal data pending verification by controller; or if there is illegitimate data processing the data subject opt for restriction of processing rather than erasure of personal data; or where the request of data subject for objection against direct marketing purposes is pending confirmation on whether the processing was based on legitimate grounds.[289] Once the restriction of processing takes place, any processing of such data in question can only be allowed in limited circumstances, either with the consent of data subject or necessary for public interests.[290] The lifting of restriction shall be informed by the controller to the data subject prior to any processing of personal data.[291]

4.5.5 Object to Processing

The PDPA recognises the right of data subject against direct marketing purposes as a right to restrict processing of personal data rather than the right to objection as per the GDPR, which is an opt-out mechanism.[292] The author views this as a mere difference in legal terminology, with a similar application. Direct marketing concerns any form of communication to advertise or market material targeted at certain individuals.[293] The author observes that the context of direct marketing suggests profiling activities, when compared with the GDPR.[294] Varying from the right to restrict processing, the PDPA is silent on providing data user with an option to refuse request of data subject to restrict processing against direct marketing, therefore, any failure of the data user to accede to such request entitles the data subject to escalate the matter to the PDPA-Commissioner in ensuring compliance however this is contingent on the

[285] PDPA, section 42(2).
[286] PDPA, section 42(3).
[287] PDPA, section 42(4).
[288] GDPR, art 18(1).
[289] ibid.
[290] GDPR, art 18(2).
[291] GDPR, art 18(3).
[292] PDPA, section 43(1); GDPR, art 21.
[293] PDPA, section 43(5).
[294] GDPR, art 4(4).

justifiability of such request.[295] If this is justifiable, the data user may be exposed to legal risks if found liable to accede to the request.[296] The GDPR similarly accords the data subject the right to object to data processing.[297] When an individual exercises this entitlement, it results in the controller and/or processor being unable to continue processing for that specific intention.[298]

The right to object to processing under the GDPR is applicable only in certain circumstances including direct marketing processing activities. Additionally, the data subject may object to processing premised on performance of a task for public interest,[299] or where it is necessary to achieve legitimate interests and this includes profiling activities.[300] Briefly, profiling is defined as automated processing of personal data to assess natural persons to predict the behaviour and other aspects of individuals.[301] In such situations, the controller shall cease any data processing altogether unless it can be shown that there are lawful grounds for processing which 'override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims'.[302] Unless there is necessary processing for public interest, any data processing activities premised on Article 89(1) of the GDPR may be objected.[303]

4.5.6 Right to Erasure

The right to erasure which is indicative of data minimisation principle under the GDPR,[304] has yet to be introduced by the PDPA. It entitles a data subject to request for his/her personal data to be erased and such request shall be immediately acceded by the controller without delay.[305] Request to erase personal data shall, upon request, be permissible in circumstances where there is no longer a need to retain data, withdrawal of consent is communicated by data subject, there is objection to processing, erasure is required to adhere to legal compliance.[306] The legal consequences to this effect renders deletion of any links, copies or replications of such data and

[295] PDPA, section 43(2); PDPA, section 43(3).
[296] PDPA, section 43(4).
[297] GDPR, art 21.
[298] GDPR, art 21(2); GDPR, art 21(3).
[299] GDPR, art 6(1)(e).
[300] GDPR, art 6(1)(f).
[301] GDPR, art 4(4).
[302] GDPR, art 21(1).
[303] GDPR, art 21(6).
[304] GDPR, art 17.
[305] GDPR, art 17(1).
[306] GDPR, art 17.

the controller is mandated to employ reasonable measures to ensure erasure of such data.[307] The only limitation forbidding enforcement of such right to erasure is the presence of an overriding public interest, legal obligations, or for archiving or research purposes.[308] The EDPB guided that this is an indispensable right which shall not be tedious in execution by data subject whenever required.[309]

4.5.7 Data Portability

As of date, the right to data portability is under evaluation by the PDPA-Ministry.[310] Based on the GDPR, this right entitles the data subject to enable the direct transfer of their personal data to another controller in a structure that is systematic, commonly employed, and machine-readable subject to two conditions.[311] Firstly, the basis for processing of personal data is consent or it is necessary to meet contractual obligations and secondly, automated methods are used for processing.[312] The right to data portability complements the access right since it permits data subject to acquire and reuse personal data, and also opt to have it transmitted to another service provider.[313] The legal rights accorded to data subject by the first controller shall not be prejudiced by the election of right to data portability.[314]

4.5.8 Rights pertaining to Automated Individual Decision-making and Profiling

The PDPA has yet to follow the steps of the GDPR to cater to the right to automated individual decision-making including profiling which results in legal repercussions or substantially impacts data subject.[315] There are three exceptions to this; firstly, the decision-making is necessary to enter or fulfil a contract.[316] Secondly, the decision is authorised under laws along with safeguards to uphold interest of data subjects.[317] Lastly, there is explicit consent by data subject to automated decision-making.[318] For the first and third exceptions, appropriate mechanisms must be employed to maintain their prerogative.[319] Any automated decision-

[307] GDPR, art 17(2).
[308] GDPR, art 17(3).
[309] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141) ch 3.
[310] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18) 4.
[311] GDPR, art 20(1); GDPR, art 20(2); GDPR, recital 68.
[312] GDPR, art 20(1).
[313] Article 29 Working Party, 'Guidelines on the right to data portability' (European Commission, 5 April 2017) 5 <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 15 August 2023.
[314] ibid.
[315] GDPR, art 22(1).
[316] GDPR, art 22(2)(a).
[317] GDPR, art 22(2)(b).
[318] GDPR, art 22(2)(c).
[319] GDPR, art 22(3).

making may involve sensitive personal data provided there is explicit consent obtained or where processing is for public interest so long appropriate measures are established.[320]

4.5.9 Right to complaint and seek legal recourse

Enforcement mechanisms are imperative as it provides the data subject a legal avenue to pursue any alleged data breach and an assurance of accountability from controller and/or processor if found liable. A data subject may, where necessary, file a written complaint directly to the PDPA-Commissioner and specify the details of complaint for review.[321] The investigation will be carried out by the PDPA-Commissioner who will decide the merits of the complaint, i.e. to proceed or dismiss the investigation.[322] There are no other legal recourse available for the data subject, save and except by through a written complaint.[323] An alternative is for the distressed data subject to consider initiating civil proceedings against data user under common law,[324] however in respect of prosecution proceedings, this falls strictly within the prerogative of the public prosecutor.[325]

The GDPR take a position that is intricate and pro data subjects in terms of the enforceability legal recourse. It is mandated on the supervisory authority to investigate any complaints filed by the data subject with the supervisory authority and to inform complainant of the progress and outcome of complaint, failing which the data subject is entitled to seek viable legal redress against the supervisory authority in the member state court of the establishment of supervisory authority.[326] Further, the supervisory authority shall apprise the complainant of any possibility of legal remedies available to address the complaint.[327] The data subject shall, in addition to the right to remedy against a supervisory authority for any non-fulfilment of obligation under Article 77,[328] shall have right to pursue legal action against controller and/or processor for any

[320] GDPR, art 22(4).
[321] PDPA, section 104.
[322] PDPA, section 105.
[323] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18) 8.
[324]Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18) 8; Baker McKenzie, 'Penalties for Non-Compliance' (Baker McKenzie, 30 December 2022) <https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/malaysia/topics/penalties-for-non-compliance> accessed 15 August 2023.
[325] PDPA, section 134.
[326] GDPR, art 77(1); GDPR, art 77(2).
[327] GDPR, art 77(2); GDPR, art 78.
[328] GDPR, art 78.

purported violation of the GDPR which can be instituted either at the habitual residence of data subject or the establishment of the controller and/or processor.[329]

4.6 Evaluation of Malaysia in Achieving Adequacy

The author had previously outlined the guidelines provided by A29WP which serves to set out the minimum requirements to be satisfied by any third jurisdiction with intention to explore or consider an adequacy decision with the EU. To encapsulate, there are three broad aspects to be considered. The third country should have a system which prescribes the basic data protection principles embedded in Articles 5 and 6 of the GDPR,[330] accord legal rights such as right to access, rectification, erasure and objection.[331] The second requirement is to cater to specific categories of processing such as sensitive personal data, direct marketing and automated decision making and profiling.[332] The third requirement is to ensure there is an effective procedural and enforcement avenue, for instance, the appointment of a competent and independent supervisory authority, accountability, and judicial reliefs available to individuals.[333]

The assessment on whether the PDPA would fulfil the criteria set by the GDPR is guided by the EDPB: firstly, the author submits that although the PDPA does not exactly mirror the legal terminology of the GDPR,[334] the data protection principles embedded in the PDPA bear striking resemblance to the GDPR prescribed in its Articles 5 and Article 6 whereby both frameworks share the same legal bases for a legitimate processing.[335] Further, the author observes that the PDPA contains a rather comprehensive list of rights accorded to data subjects, however, this observation may change considerably as its counterpart is the GDPR which has a broader and specific category of rights avail to data subjects, with the main distinctive features being that the PDPA has yet to introduce the right to erasure, right not to be subjected to automated decision-making and profiling.

Regarding the second requirement, there is a higher threshold to be complied with prior to the processing of sensitive personal data. Such processing is prohibited unless it falls within the

[329] GDPR, art 79.
[330] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141) ch 3.
[331] ibid.
[332] ibid.
[333] ibid.
[334] ibid.
[335] ibid.

category prescribed in Article 9 or 10 of the GDPR in circumstances where data subject provides explicit consent for processing, or where there is necessity to process such special categories of personal data, or where the processing is carried out under the control of public authorities.[336] In this aspect, the PDPA has a dedicated provision under Section 40 of the PDPA which acknowledged that a higher standard of protection is required hence the imposition of higher threshold as seen in the GDPR. As for direct marketing purposes, data subject must be permitted the right to object to processing for such reasons at no cost.[337] It is noteworthy that the PDPA allows data subjects the right to restrict processing of personal data where there is a likelihood of damage or distress from occurring or in situations of direct marketing although it is not explicitly regarded as 'right to object'.[338] The evaluation of these rights under both jurisdictions suggests there is a different approach taken whereby the PDPA only permits the data subject the right to restrict processing provided the personal data in question were processed outside the legal bases in Section 6 of the PDPA and subsequently, the data user has the option to decide whether to restrict the processing, subject to a possible review by the PDPA-Commissioner on the data user's decision.[339]

The third requirement is that there shall be an effective procedural and enforcement avenue. It is intended to keep a form of accountability and transparency when it concerns the observation and compliance of the third country's data protection legislation.[340] It is also important to ensure good compliance of the data protection system in the third country, by its controller and/or processor.[341] Accountability principle, as portrayed in Article 5(2) of the GDPR, is of paramount importance, as it links to the essence of data protection obligations imposed on the controller and/or processor in carrying out data protection impact assessments, appointment of data protection officer and making sure that the data protection mechanisms by way of design and by default are in place.[342] The author observes there is accountability principle in place under the PDPA with regards to the obligations of the data user (equivalent to controller under the GDPR), however the same is not extended to the data processor at this juncture. Lastly, the implementation of an effective redress mechanisms should be enforced in the third country, aligned with the GDPR, to ensure that an individual may in a timely and effective manner

[336] GDPR, art 9; GDPR, art 10.
[337] GDPR, art 21(2).
[338] PDPA, section 42; PDPA, section 43.
[339] PDPA, section 42(4).
[340] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141) ch 3.
[341] ibid.
[342] ibid.

pursue their legal rights over an infringement or unlawful interference or compliance with their data protection rights.[343] The author opines that there is scope of improvement for the PDPA in this aspect as data subjects only have the means to file a complaint to the PDPA-Commissioner, however there is no legal avenue for the aggrieved data subject to initiate direct proceedings against the data user or the PDPA-Commissioner, as would been widely available under the GDPR. Any initiation of proceedings will be subject to the consent of the public prosecutor beforehand. Despite some shortfalls in the PDPA, the author asserts that, holistically, it remains a comprehensive legislation that has remained closely aligned with the fundamental principles of the basic PDP which permits opportunities for enhancement.

[343] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141) ch 3.

[F] CHAPTER 5: APPROPRIATE SAFEGUARDS

If a decision has yet to be made in support of an adequacy decision in favour of Malaysia, a controller and/or processor in the EU/EEA ("**Data Exporter**") may utilise the alternative transfer mechanism of appropriate safeguard.[344] The precondition is the implementation of an appropriate safeguard under Article 46 of the GDPR, and that the enforceable legal entitlements are readily accessible to data subjects.[345] It is crucial that the level of data protection must be guaranteed during the transmission to third countries or international organisations.[346] Though it is inconclusive, appropriate safeguard are possibly the next best alternative after an adequacy decision by the EC for CBPDT for plausible reason that in an adequacy decision, there is a four-tier process whereby the legislative and political aspects of the third countries are being evaluated.[347] To outline, the GDPR categorised SCC, approved code of conduct, binding corporate rules, approved certification mechanisms and legal instruments between public institutions under the umbrella of appropriate safeguard.[348] These appropriate safeguards are multifaceted data protection measures employed by controller and/or processor using technology and organisational commitments as framework to compensate the shortfall of data protection level in third countries.[349] This paper will provide a comprehensive explanation of the various appropriate safeguards in this chapter.

5.1 Standard Contractual Clauses

Among the diverse appropriate safeguard measures, SCC is widely relied upon by business organisations for CBPDT.[350] It is a series of pre-approved standard template by the EC which can be utilised by private entities, be it controller or processor as a layer of protection when entering into agreement with counterparty and this applies to data transfer within and outside

---

[344] GDPR, art 46.
[345] GDPR, art 46(1).
[346] Schrems II, paras 92 and 93.
[347] GDPR, art 46(1); European Commission, 'Adequacy Decisions' (n 143); Data Protection Commissioner, 'Transfers of Personal Data to Third Countries or International Organisations' (n 145).
[348] GDPR, art 46(2).
[349] GDPR, recital 108; Schrems II, paras 134 – 135; Laura Bradford, Mateo Aboy and Kathleen Liddel, 'Standard contractual clauses for cross-border transfers of health' (2021) 8 Journal of Law and the Biosciences 1, 3 <https://doi.org/10.1093/jlb/lsab007> accessed 15 August 2023; European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 15 August 2023.
[350] Nigel Cory, Ellysse Dick and Daniel Castro, 'The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade' (Information Technology & Innovation Foundation, 17 December 2020) <https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade/> accessed 15 August 2023.

the boundaries of EU/EEA.[351] Primarily, the SCC was designed to ensure consistent application throughout all third countries independent of varying scales of data protection in respective third countries.[352] The SCC constitutes contractual clauses which sets a baseline level of protection which must be strictly adhered to by controller and/or processor, however, the contracting parties are afforded the liberty to expand the scope to reinforce data protection provided there are non-conflicting or non-contradiction clauses with the SCC template.[353] In fact, the introduction of additional supplementary measures using contractual clauses to strengthen protection by either controller or processor are most welcomed.[354]

This paper had earlier set out in ***Chapter 3.2.2*** on how the Schrems case series had illuminated on the application of CBPDT using the transfer tools stipulated in Chapter V of the GDPR. The decision in Schrems II had heavily shaped the approach taken by the EC in relation to the SCC, which led to the birth of two revised sets of SCC by the EC after considering the viewpoint of EDPB and European Data Protection Supervisor ("**EDPS**").[355] The first set of the revised SCC template initiated applies to the controller and/or processor within the ambit of the EU/EEA ("**SCC EU**") while the other template is specifically tailored for international data transfers to third countries and/or international organisations ("**SCC Third Country**").[356] These SCC templates were intended to ensure coherence and introduce 'one single entry point' to accommodate types of CBPDT in addition to serving as a pragmatic toolbox to assist

[351] Directorate-General for Justice and Consumers, 'The New Standard Contractual Clauses – Questions and Answers' (*European Commission*, 4 June 2021), 4 <https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf> accessed 15 August 2023.
[352] Schrems II, para 133.
[353] GDPR, recital 109.
[354] ibid.
[355] Schrems II; Directorate-General for Justice and Consumers, 'Standard contractual clauses for controllers and processors in the EU/EEA' (*European Commission*, 4 June 2021) <https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en> accessed 15 August 2023; Directorate-General for Justice and Consumers, 'The New Standard Contractual Clauses – Questions and Answers' (n 351); Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance) OJ L 199/18 ("**SCC EU**"); Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) OJ L 199/31 ("**SCC Third Country**"); European Commission, 'European Commission adopts new tools for safe exchanges of personal data' (*European Commission*, 4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847> 15 August 2023.
[356] Directorate-General for Justice and Consumers, 'Standard contractual clauses for controllers and processors in the EU/EEA' (n 355); Directorate-General for Justice and Consumers, 'Standard contractual clauses for international transfers' (*European Commission,* 4 June 2021) < https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en> accessed 15 August 2023.

organisations in meeting the legal requirements arising from the CJEU's decision in Schrems II.[357] The EC appreciates the different variables involved in CBPDT and introduced four distinctive modules in an unified template under the SCC Third Country.[358] It is noteworthy that there are varying degrees of responsibilities mandated on the controller as opposed to the processor and this is evident in module 1 and 3 of the SCC Third Country.[359]

The CJEU in Schrems II suggests that the SCC are invalid if there are absence of any supplementary measures to compensate the deficiencies of the third country's legislations.[360] Hence, it means that where the findings reveal the deficiency of third countries legislations to which data is exported, it is recommended that data exporters establish supplementary measures to ensure the objectives of EU are consistently and this can be a blend of multiple measures.[361] Although the decision of Schrems II is silent on what constitutes adequate supplementary measures, the EDPB provided some insight on this in its guidelines.[362] Based on the GDPR, the Data Exporter may utilise the security principles and protection by way of design and by default as supplementary measures which requires the assessment of risk in advance.[363]

Under the SCC, the responsibility to ensure that CBPDT is adequately protected by the laws of third country is on the Data Exporter, or the supervisory authority if the Data Exporter fails to examine the same and these shall be conducted based on individual assessment.[364] The author views that the shift in responsibilities to the controller and/or processor demonstrates the accountability principle.[365] When assessing the CBPDT, if the evaluation reveals that the supplementary measures are insufficient to guarantee such protection, the data transmission should either be suspended or terminated and more so, when the laws of third countries are in conflict with the EU laws.[366] Any assessment and establishment of the supplementary measures

[357] European Commission, 'European Commission adopts new tools for safe exchanges of personal data' (n 355).
[358] SCC Third Country.
[359] ibid.
[360] Schrems II, paras 134 – 135; Bradford, Aboy and Liddel (n 349) 2.
[361] Schrems II, para 134; European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (n 349) 4.
[362] European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (n 349) 4.
[363] GDPR, Article 25; GDPR, Article 32; Axel Voss (n 151) 31.
[364] Schrems II, para 134; Schrems II, AG Opinion, para 126.
[365] GDPR, art 5(2).
[366] Schrems II, para 135.

shall be recorded and easily made available for sight of supervisory authority, where required.[367]

Alex Voss likened the shift in responsibility to Data Exporter to assess individual CBPDT and decide which is the appropriate approach and whether supplementary measures are required as a 'mini-adequacy' decision' and opines that this approach is neither ideal nor feasible.[368] There are scholars who opined that the CJEU had undermined the use of appropriate safeguards and construed it rather narrowly in that the SCC used are to guarantee a level equivalent to the Charter.[369] Such expectations premised on the SCC entered between private corporation or organisations is unattainable for reasons that the contractual obligations do not bind the government of that third country, hence it may not prove feasible to address any deficiencies in the laws of third countries.[370] The probable outcomes of the Schrems II decision is an outright restriction on CBPDT with third countries with weak or inadequate data protection laws in place, thus deterring international trade opportunities.[371] On one hand, the SCC may appear to be an ideal mechanism to accelerate CBPDT, however, the decision in Schrems II may have complicated it further. Regardless, this paper seeks to also evaluate the ASEAN Model Contractual Clause ("**MCC**") which was jointly developed between the EU and ASEAN in the next subchapter.

5.1.1 SCC v MCC

The EU-ASEAN partnership acknowledges the growing demand for modern data protection clauses such as the SCC and had collaborated to introduce MCC by using the SCC as a paragon.[372] The introduction of the MCC is intended to support global trade as well as to facilitate international businesses in the compliance of CBPDT and relevant legislation across the EU and ASEAN.[373] The MCC, finalised in January 2021, is a reflection of the older version

[367] GDPR, art 5(2); GDPR, art 24(1).
[368] Axel Voss (n 151) 31.
[369] Bradford, Aboy and Liddel (n 349) 15.
[370] ibid.
[371] ibid.
[372] ASEAN, 'ASEAN Model Contractual Clauses for Cross Border Data Flows' (ASEAN, January 2021) <https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf> accessed 15 August 2023; Directorate-General for Justice and Consumers, 'Joint Guide to ASEAN Model Contractual Clauses and EU Standard Clauses' (*European Commission*, 24 May 2023) <https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf> accessed 15 August 2023.
[373] ASEAN, 'ASEAN Model Contractual Clauses for Cross Border Data Flows' (n 372); Directorate-General for Justice and Consumers, 'Joint Guide to ASEAN Model Contractual Clauses and EU Standard Clauses' (n 372).

of the SCC introduced in line with the Directive which may be included by business organisations on a voluntary basis, for CBPDT within the ASEAN member states.[374] The MCC was adopted during the ASEAN Digital Ministers' meeting whereby Malaysia was one of the participating members of ASEAN which approved the use of MCC as well as the use of ASEAN Data Management Framework ("**DMF**").[375] It is significant to note that the DMF serves as a guide for private businesses in the establishment of a data management system which aid on the governance and regulation.[376] The EU and ASEAN had issued a guide to illuminate businesses across the EU and ASEAN region of the workings and features of the MCC and the SCC and promote adherence with applicable laws and regulations.[377] The most distinctive features of the MCC and the SCC is that the former was introduced prior to the decision of Schrems II, hence they have a narrower coverage only in respect of controllers' obligations.[378] Although Malaysia had publicly supported the use of MCC, it remains uncertain whether the MCC has been applied in practice within the ASEAN region given that these are templates for the inclusion into private and confidential contractual agreements between private entities.

Graham Greenleaf analysed the legal positions in the ASEAN member states and found that there is non-uniformity in the approach taken by each of the respective member states, with varying degrees of level of data protection.[379] Malaysia, Singapore and Philippines have their data protection laws in place, however Laos and Myanmar for example, do not have significant protection framework.[380] Given the conflicting approach of the ASEAN member states, there is a lack of effectiveness in any form of the MCCs, whether in the respective jurisprudence of

[374] Baker McKenzie, 'ASEAN: Adopting the ASEAN Model Contractual Clauses for cross-border data transfers' (*Baker McKenzie*, 2 November 2021) <https://insightplus.bakermckenzie.com/bm/data-technology/asean-adopting-the-asean-model-contractual-clauses-for-cross-border-data-transfers_1> accessed 15 August 2023; Bernama, 'Saifuddin: Malaysia committed to helping Asean secure data flow, enhance cyber security' (*New Straits Times*, 21 January 2021)<https://www.nst.com.my/news/nation/2021/01/659340/saifuddin-malaysia-committed-helping-asean-secure-data-flow-enhance-cyber> accessed 15 August 2023.
[375] ASEAN, 'ASEAN member states' (*Association of Southeast Asian Nationals*' <https://asean.org/member-states/> accessed 14 June 2023; Department of Personal Data Protection,
Asean Data Management Framework (Dmf) And Asean Model Contractual Clauses For Cross Border Data Flows (MCCs)' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/assets/2021/11/Guidelines-for-DMF-and-MCC-ASEAN.pdf> accessed 15 August 2023
[376] Pillai and Yong (n 24).
[377] Directorate-General for Justice and Consumers, 'Joint Guide to ASEAN Model Contractual Clauses and EU Standard Clauses' (n 372) 6.
[378] ibid, 8.
[379] Greenleaf, G 'ASEAN Model Contractual Clauses: Low and ambiguous data privacy standards' (2021) 174 Privacy Laws & Business International Report, 22-24.
[380] ibid.

each member states or international agreements within ASEAN.[381] In fact, the MCCs are a 'voluntary standard' to provide mere guidance on factors to be considered when conducting data transfer and this is unlike the EU's SCCs which promotes uniformity across the region.[382] Notwithstanding the aforesaid, the MCC is regarded to be more suited to certain countries which has yet to implement any national data protection legislation or has a rather 'low level of standard protection in place'.[383]

5.1.2 Evaluation

In considering the PDP landscape of Malaysia pertaining to the adoption of the SCC, the author opines that it is feasible for the private sectors and organisations to utilise SCC when entering contracts with international businesses. Considering the practical aspect, the SCC which are preapproved templates are effective, convenient and user-friendly for internationally based contracting parties to incorporate to their contract and expound the obligations and rights where allowed.[384] Based on the participation and approval of Malaysia in the adoption of the MCC for its use within the ASEAN businesses, the author submits that Malaysia is receptive to the notion of adopting the MCC. After all, the MCC was inspired by the SCC and the current version of the SCC was introduced to fortify the contractual obligations between controllers and processors in assorted contexts, having in mind, the development of Schrems cases.[385] The author adds that the implementation of the MCC (or SCC) in practice would be in the best interest of private organisations in Malaysia, not only in terms of its legislative framework, but also in terms of economic perspective. In terms of its enforcement. Hence, the author proposes for the enactment of the model clauses in the PDPA on all data user and/or processors inclusive of the private sectors. Additionally, the author recommends that the Malaysian policymakers consider incorporating these contractual responsibilities into current legal framework, for example, the PDPA as well as the Companies Act 2016 in Malaysia, to ensure uniformity in the enhancement the individuals' personal data right to provide assurance and certainty to data subjects.

[381] Greenleaf, G 'ASEAN Model Contractual Clauses' (n 379) 22-24.
[382] ibid; ASEAN, 'ASEAN Model Contractual Clauses for Cross Border Data Flows' (n 372) 4.
[383] Greenleaf, G 'ASEAN Model Contractual Clauses' (n 379) 22-24.
[384] Directorate-General for Justice and Consumers, 'The New Standard Contractual Clauses – Questions and Answers' (n 351) 4.
[385] ASEAN, 'ASEAN Model Contractual Clauses for Cross Border Data Flows' (n 372).

5.2 Binding Corporate Rules ("**BCR**")

The GDPR also introduces another mechanism under appropriate safeguards for CBPDT known as BCR.[386] The author aims to explore the operations of BCR and assess whether it is beneficial to emulate by the PDPA. The BCR is a set of policies observed by a Data Export in respect of any CBPDT among a group of entities involved in a joint economic activity.[387] Aligned with the consistency and cooperation mechanisms, the competent supervisory authorities pre-approved the draft BCR prior to utilisation of the same within a group of companies.[388]

Of note, certain requirements must be fulfilled before a draft BCR may be approved. The BCR shall be legally binding on every corporate members within an organisation and the application of BCR shall extend to bind their employees as well.[389] The stipulation of legal rights accorded to data subject must be provided in the BCR and shall, at a minimum, contain corporate information and details on the processing such as organisation chart, the characteristics and intended use of data to be transferred, the list of recipient, legal entitlement of data subject, complaint procedures and transfer mechanisms established within the group to ensure compliance of BCR.[390] At the time of filing the application for approval, the applicant must nominate a supervisory authority which acts as a liaison party in the communication relating to the application and provide justification for the same.[391] Additional information may also be submitted regarding the location of the headquarter office of the group of companies, the location of the company within the group which is responsible for data protection duties and the member state which the CBPDT usually takes place.[392] Where the draft BCR is deemed satisfactory by the supervisory authority, it will be circulated for review by the EDPB which will provide a non-binding opinion.[393] The number of supervisory authorities involved in the approval process is subject to the total number of entities within the group undertaking.[394]

---

[386] GDPR, art 47.
[387] GDPR, art 4(20).
[388] GDPR, art 47(1); GDPR, art 63.
[389] GDPR, art 47(1); GDPR, art 63(1).
[390] GDPR, art 47(1); GDPR, art 46(2).
[391] Article 29 Data Protection Working Party, 'Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR' (European Commission, 11 April 2018) <https://commission.europa.eu/document/download/dec4329d-951e-41e2-82e9-b0ade63c0d8b_en> accessed 15 August 2023.
[392] Article 29 Data Protection Working Party, 'Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR' (n 391).
[393] GDPR, art 64.
[394] Article 29 Data Protection Working Party, 'Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR' (n 391).

5.2.1 Analysis of BCR

At the outset, Malaysia is part of the Asia-Pacific Economic Cooperation which had endorsed the use of Cross-Border Privacy Rules Mechanism ("**CBPR**").[395] At the time of writing this article, Malaysia has yet to adopt the CBPR, however had shown interest to embrace the same.[396] Briefly, the CBPR bears similar structure as the EU's BCR which is a 'government-backed data privacy and security certification program' brought about in 2005 and endorsed in 2011 was initially intended as a regional transfer tool intra-APEC members.[397] It is suggested that the CBPR sets the absolute minimum to support the CBPDT, however, it may be further enhanced to replicate GDPR-like principles.[398] Given that the GDPR is a global standard, the author finds it may be more appropriate and effective for Malaysia policymakers to amend the PDPA in line with the GDPR as it would naturally be one which complies with CBPR. The author foresees that the adoption of this transfer tool will benefit private businesses or organisations, particularly multinational companies, or conglomerate businesses. The author submits that given the fluidity of information which flows easily and almost instantaneously, there is a pressing necessity for the adoption of the BCR to introduce by way of legislation in the Companies Act 2016 for uniform adherence on global corporations with a corporate or branch office in Malaysia. Similar to the SCC, the BCR will assist in the regulation of PDP.

5.3 Certification Mechanism ("**Certification**")

The policymaker may consider the implementation of endorsed certification and data protection seals and marks for CBPDT.[399] The GDPR mandates the issuance of certification

---

[395] Asia-Pacific Economic Cooperation, 'Member Economies' (*Asia-Pacific Economic Cooperation*) <https://www.apec.org/About-Us/About-APEC/Member-Economies> accessed 15 August 2023.
[396] Mark Chan, 'Digital Payments, Data Regulations, and AI as Most Promising Areas for Digital Economy Collaboration' in Paul Cheung and Xie Taojun (eds), *The ASEAN Digital Economy: Towards an Integrated Regional Framework* (Routledge 2024) <https://books.google.ie/books?hl=en&lr=&id=XEDJEAAAQBAJ&oi=fnd&pg=PA76&ots=C_aOf38yUH&sig=dho0sXRnLVgNVmvGk9KM6z39NKw&redir_esc=y#v=onepage&q&f=false> accessed 15 August 2023; Centre for Information Policy Leadership, International Data Flows: Cross Border Privacy Rules, Privacy Recognition for Processors, and Global CBPR and PRP (*Centre for Information Policy Leadership*, July 2023) 5 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cbpr_prp_faq_updated_july23.pdf> accessed 15 August 2023.
[397] Centre for Information Policy Leadership (n 396) 2. <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cbpr_prp_faq_updated_july23.pdf> accessed 15 August 2023; María Vasquez Callo-Müller, 'GDPR and CBPR: Reconciling Personal Data Protection and Trade' (2018) APEC Policy Support Unit POLICY BRIEF No. 23 <https://www.apec.org/docs/default-source/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade/218_PSU_Policy-Brief_GDPR_CBPR.pdf> accessed 15 August 2023.
[398] Callo-Müller (n 397).
[399] GDPR, art 46(2)(f).

under the prerogative of appointed certification bodies or competent supervisory bodies subject to fulfilment of certain conditions.[400] Having a certification does not in any way narrow the scope of responsibilities of controller and/or processor under the GDPR however it serves as a validation tool to assure the establishment of appropriate safeguards.[401] The certification is a voluntary process signed up by controller and/or processor to implement the safeguards accompanied by rights and remedies to data subjects.[402] The EDPB clarifies that the application of certification and marks should be filed by controller and/or processor established in third countries ("**Data Importers**").[403] This does not exclude the Data Exporters who intends to opt for such tools for processing of personal data within EU.[404] There are a certain set of requirements to be met by Data Exporters, mainly to specify the validity and coverage of certification, the specific transaction for use and take into account any onward transfers.[405] The author opines there is a greater accountability on Data Exporters to ensure certification mechanism is effective for third country data transfer.[406] There is no hindrance for the Data Exporter to rely on the assessment of certification bodies in third countries on examination of adequacy of existing measures or whether additional measures are required.[407]

The use of certification, seal or marks enhances the transparency principle, granting data subjects immediate assurance and quick assessment of the measures used when purchasing goods or engaging services from suppliers.[408] The validity of the issued certification is for a period of three years, which may be renewed and withdrawn subject to the fulfilment of the conditions being met by the data controller and/or data processor.[409] In fact, the GDPR stipulates that there should be cooperation and efforts made at the EU level among the EU member states, EDPB, the EC and supervisory authorities in the establishment of data protection certification mechanisms, data protection seal and marks.[410] Since the enactment of GDPR in 2018, GDPR-CARPA is the first certification mechanism introduced by the national

[400] GDPR, art 42(5); GDPR, art 43; GDPR, art 58(3).
[401] GDPR, art 42(2); GDPR, art 24(3).
[402] GDPR, art 42(2).
[403] European Data Protection Board, 'Guidelines 07/2022 on certification as a tool for transfers' (*EDPB*, 14 February 2023) 9 <https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf> accessed 15 August 2023.
[404] European Data Protection Board, 'Guidelines 07/2022 on certification as a tool for transfers' (n 403) 9.
[405] European Data Protection Board, 'Guidelines 07/2022 on certification as a tool for transfers' (n 403) 10.
[406] European Data Protection Board, 'Guidelines 07/2022 on certification as a tool for transfers' (n 403) 10.
[407] European Data Protection Board, 'Guidelines 07/2022 on certification as a tool for transfers' (n 403) 10.
[408] GDPR, recital 100.
[409] GDPR, art 42(7).
[410] GDPR, art 42(1).

supervisory authority of Luxembourg.[411] The author views that the certification scheme is a relatively long process having regard to the audit processes required to fully understand the ecosystem and framework of a particular state before rolling out a suitable certification mechanism.[412]

5.3.1 Assessment of Certification

Having regard to the legal system in Malaysia, the author views it is uncertain on the feasibility of adopting and implementing the certification under the PDPA especially with the deficiencies to be highlighted in the PDPA in ***Chapter 7.2***. The author considers that whilst it may be feasible for the implementation of certification framework, this may be economically impracticable in terms of cost and time. This paper has seen that by far, with the GDPR being in operation for at least five years, Luxembourg is the only country which has successfully implemented the certification mechanisms.[413] The author notes that the process for certification shares similarity to adequacy whereby it involves audit processes on the interested private businesses or organisations.[414] Further, the author views that there may be a potential overlap between the adequacy decision and certification mechanism whereby assessment would be required, hence it may be more viable to opt for the adequacy decision mechanism which has seen more chances of success in the issuance of decisions in favour of 15 jurisdictions.

5.4 Approved Code of Conduct

The GDPR permits use of approved code of conduct ("**COC**") which can either be approved by the supervisory authorities,[415] or approved by the EC in situations where it involves processing activities in more than one Member States.[416] The EDPB enlightened that the COC should encompass the nature of data transfer, the basic principles, accountability measures, complaint handling procedures, as well as a warranty from the third-party controller and/or processor in its adherence to the COC and implementation of supplementary measures for such

[411] European Data Protection Board, 'The CNPD adopts the certification mechanism GDPR-CARPA' (*EDPB*, 27 June 2022) <https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en> accessed 15 August 2023.
[412] European Data Protection Board, 'The CNPD adopts the certification mechanism GDPR-CARPA' (n 411).
[413] ibid.
[414] ibid.
[415] GDPR, art 40(5).
[416] GDPR, art 40(9).

adherence.[417] Unless the COC pertains to processing activities in several Member States, the supervisory authority has the jurisdiction to assess whether the code of conduct contains sufficient safeguards and approve and publish the same in the register.[418] Reviews of the COC concerning transmission to third countries would first require the opinion of the EDPB for the EC to consider simultaneously before approval is granted by way of implementing act.[419] There shall be mechanisms in place to ensure that mandatory observation of the compliance of the COC be carried out in accordance with the GDPR by an accredited body with relevant expertise pursuant to the EDPB guideline.[420] It is important to note that the processing activities carried out by public authorities are exempted from mandatory monitoring.[421] A feature of the COC is that it may be tailored to suit different needs, subject to the context, either general application of GDPR,[422] or for CBPDT.[423] Essentially, the COC must be legally binding and enforceable in line with the EU law and may be enforceable by data subjects as third-party beneficiaries.[424]

It would be beneficial for the Data Importer to have a better grasp of the implementation of appropriate safeguards that are specific to the respective business needs.[425] The Data Exporter may rely on the compliance of the data importers in third countries to demonstrate adherence to the code of conduct.[426] The BCR imposes a transfer of responsibility in respect of the compliance of the transfer of data pursuant to the GDPR, which shifts from the Data Exporter to the Data Importer provided there are in place legal documents to ensure the continuous protection of data subjects' rights and implementation of basic principles.[427] Whilst there is no specific requirement of the location of the organisation intending to utilise the COC within the

[417] GDPR, art 40(2); GDPR, art 28; European Data Protection Board, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (*European Data protection Board*, 22 February 2022), 13-14 <https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf> accessed 15 August 2023.
[418] GDPR, art 40(5); GDPR, art 40(6).
[419] GDPR, art 40(9).
[420] GDPR, art 40(4); GDPR, art 41(1); GDPR, art 41(2); European Data Protection Board, 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Version 2.0' (European Data Protection Board, 4 June 2019) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf accessed 15 August 2023.
[421] GDPR, art 41.
[422] GDPR, art 40(2).
[423] GDPR, art 40(3).
[424] GDPR, art 28; European Data Protection Board, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (n 417) 11.
[425] European Data Protection Board, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (n 417) 6.
[426] ibid, 3.
[427] ibid, 7-8.

EU region, it is a pre-requisite that the organisation pledge a high level of commitment through a contract towards the adherence of GDPR and ensure it is always upheld.[428]

As briefly discussed earlier on the latest introduction of the general PDPA COP which binds data users which have yet to be subjected to a specific PDPA COP applicable to selected sectors including aviation[429] and utilities[430], the author observes that there is striking resemblance in the workings of the PDPA-COP in comparison to the code of conduct under the GDPR. At the outset, the author submits that the PDPA-COP strictly applies to classes of data users required to be registered under the law and this is a unique feature to regulate compliance.[431] Any failure to adhere to the PDPA-COP will result in fine and/or imprisonment.[432] The evaluation of the various PDPA-COP reveals that any CBPDT is subject to the application of Section 129 of the PDPA, although the aviation and the banking and healthcare sectors stipulates additional practical steps as guide.[433] For example, carrying out due diligence and ensure that the data transfers are premised on the grounds under the law.[434]

5.4.1 Evaluation of COC

The author submits that Malaysia had prepared a similar framework of the code of conduct prescribed in the GDPR known as the PDPA-COP. Although it is underway in its prescription as a comprehensive CBPDT tool at this juncture, yet the author views that assurance can be found in the fact that with the PDPA being revised to adopt the COC mechanism and cater to CBPDT, eventually, the existing PDPA COP can be further elaborated to meet the specific needs to enhancing measures for international transfer. The PDPA-COP shall be read together with the PDPA, hence any enhancement of the PDPA will consequentially reflect a change in

[428] GDPR, Article 28; European Data Protection Board, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (n 417) 11.
[429] Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Malaysia Aviation Sector' (*Official Portal of Department of Personal Data Protection*, 21 November 2017) <https://www.pdp.gov.my/jpdpv2/tata_amalan/the-personal-data-protection-code-of-practice-for-the-malaysia-aviation-sector/> accessed 15 August 2023.
[430] Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Utilities Sector (Electricity' (*Official Portal of Department of Personal Data Protection*, 23 June 2016) <https://www.pdp.gov.my/jpdpv2/tata_amalan/the-personal-data-protection-code-of-practice-for-the-utilities-sector-electricity/> accessed 15 August 2023.
[431] PDPA, Division II of Part II; PDPA, Division III of Part II; Walters, Trakman and Zeller (n 24) 207-209.
[432] PDPA, section 29.
[433] PDPA, section 129(1); Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Malaysia Aviation Sector'(n 429) 52-53; Department of Personal Data Protection, 'Personal Data Protection Code of Practice for the Banking and Financial Sector' (n 42).
[434] ibid.

the PDPA-COP.[435] The author observes that only selected sectoral PDPA-COP have elaborated on the pragmatic steps to be taken if CBPDT is carried out,[436] hence the author submits that there should be a uniform application reflected in all the PDPA-COP, regardless of it being sectoral or general, and the policymakers should consider addressing the issue on CBPDT.

5.5 Data Transfer Mechanisms between Public Authorities

The GDPR introduced two avenues for data transfer explicitly between public authorities in the EU and third countries. The first avenue is legally binding and enforceable instrument[437] while the second avenue is clauses to regulate administrative arrangements.[438] They are practical CBPDT tools in that they apply to situations exempted from adequacy decisions; for example, in Japan whereby the adequacy adopted only covers private sectors and not the public sector.[439] The safeguards are not effective against commercial transactions where one of the contracting parties is either a private corporation or individual.[440]

Any transfers or onward transfers between public authorities shall comply with the EU law, wherein they should not go beyond what is considered necessary and proportionate.[441] Premised on Schrems II, the EU public authority takes on the obligation to assess the strength of protection of third country and identify if safeguards established in the treaty or convention are effective.[442] The requirements on providing data subject with information regarding the processing activities and legal entitlement cannot be compromised.[443] If it is not feasible to

---

[435] Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 5.
[436] PDPA, section 129(1); Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Malaysia Aviation Sector'(n 429) 52-53; Department of Personal Data Protection, 'Personal Data Protection Code of Practice for the Banking and Financial Sector' (n 42).
[437] GDPR, art 46(2)(a).
[438] GDPR, art 46(3)(b).
[439] European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies' (European Data Protection Board, 15 December 2020) 5 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf> accessed 15 August 2023.
[440] Data Protection Commission of Ireland, 'Transfers of Personal Data to Third Countries or International Organisations' (Data Protection Commission) (n 145).
[441] GDPR, art 23(1); European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679' (n 439) 13.
[442] Schrems II, para 105; European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679' (n 439) 7.
[443] European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies' (European Data Protection Board, 15 December 2020) 13 – 14 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf> accessed 15 August 2023.

assure effective judicial relief for data subject, consultation with competent supervisory authorities is necessary.[444] Data subject should be entitled to timely and effective redress mechanisms by way of complaint to the contracting public authorities of the international agreement and to the independent oversight mechanisms.[445] The judicial relief mandatorily available to data subject should include compensation in damages for any proven unauthorised processing of personal data.[446] The EU policymakers acknowledges the necessity to have an oversight mechanism with independent supervision to observe compliance of the international agreement and carry out periodic audit to ensure effectiveness and efficiency of safeguards.[447] Regular communications between contracting parties and status update reports to the independent oversight mechanisms may be beneficial to ensure adherence to EU jurisprudence.[448]

5.5.1 Analysis

The author finds that the data transfer mechanisms between public bodies are essential tools which provides assurances to the contracting party that free movement of personal data transferred are done in a secure manner and does not undermine any fundamental right of personal data protection pursuant to EU framework. However, the author views that the suitability and applicability of this mechanism in the judicial system of Malaysia hinges largely on the fact on whether the policymakers regard the necessity to extend the scope of application to public sectors. The author views that unless revision is made to remove the exclusion of public sectors from the PDPA, it may be futile to consider this mechanism at this juncture as it is contingent on a long-term binding contractual commitment between the trading nations as it allows check and balances on the operation and to ensure that legal redress mechanisms are established for enforcement.

[444] European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679' (n 439) 17.
[445] European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679' (n 439) 13-14.
[446] ibid, 14.
[447] ibid, 15.
[448] ibid.

[G] CHAPTER 6: CROSS-BORDER PERSONAL DATA TRANSFER BY WAY OF DEROGATION

Consent remains a foundational principle in the realm of data protection despite it having garnered criticisms to be discussed below.[449] The long-standing ground of processing is recognised in the jurisdictions of Malaysia and the EU. Specifically, for CBPDT, the PDPA and the GDPR necessitates the obtainment of explicit consent from data subject prior to any international data transfer for it to be a lawful transfer.[450] This chapter will briefly explore the position of the PDPA in respect of CBPDT premised on derogation and subsequently the GDPR, however, this paper will only account for use of explicit consent.

There is a general prohibition on transfer of data outside Malaysia, and there is no specified third jurisdiction provided in law permitting such transfer. However, as a means of derogation option, the PDPA recognises a CBPDT premised on either of the eight non-cumulative grounds as a lawful processing.[451] The first ground is consent, followed by necessary processing on grounds for the performance or completion of contractual obligations, legal proceedings, where data user has reasonable grounds to do so, vital and public interests.[452] Although the PDPA is silent on what constitutes consent, the PDPA-COP illuminates that consent can be in the form of a signature, verbal or action including ticking a box to indicate consent.[453]

Like the PDPA, the GDPR recognises derogation in specific circumstances.[454] Transfer based on derogations shall be applied restrictively to prevent it from being treated as a preferred method or backup choice for data transfer.[455] Derogation, in its nature, do not provide any form of security for data subjects in terms of the legal entitlement accorded by it, as such this impose a higher risk for data subjects and possibly a least favourable option when compared to either adequacy decision or appropriate safeguard mechanisms.[456] The GDPR stipulates that the EU

[449] Benjamin Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Marit Hansen et al (eds), *Privacy and Identity Management: The Smart Revolution* (Springer 2018) 111-112.
[450] GDPR, art 49; PDPA, section 129(3)(a).
[451] PDPA, section 129(3).
[452] ibid.
[453] Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 11.
[454] GDPR, art 49(1).
[455] European Data Protection Board, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' (European Data Protection Board, 25 May 2018) 4 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf> accessed 15 August 2023.
[456] European Data Protection Board, 'Guidelines 2/2018 on derogations of Article 49' (n 455) 4.

and its member states may enforce laws to restrict the methods for CBPDT in absence of any adequacy.[457] Also, there is a rigorous implementation whereby derogation shall only be allowed provided there is no repetition of CBPDT and only where it is necessary.[458] The EDPB illuminated on the 'no repetition' requirement and clarified that whilst transfer premised on derogation can occur more than once, it cannot be done as part of a routine or in situations where the data exporter and importer have a 'stable relationship'.[459] The repetitive transfers on derogation will defeat the stringent condition for imposition of transfer tools such as adequacy measures and appropriate safeguards.[460] Decisions made by authorities in third country mandating personal data disclosure from the EU can only be recognised and enforceable if the obligation originates from an international agreement, failing which they fall outside the scope of lawful grounds for international data transfers.[461]

Briefly, there are seven grounds for processing of personal data in the context of CBPDT such as explicit consent of data subject, necessary grounds justifying derogation which entails transfers for purposes of meeting the performance of contract, the interest of data subject, public interest, vital interest or for purposes of legal actions.[462] In respect of processing premised on legitimate interests, the data involved shall be restricted to the necessary information and not in its entirety.[463] It is crucial to also note there are some processing grounds which are not applicable to processing by public authorities.[464]

To unpack the definition of consent for purposes of data transfer, there are four key criteria which constitutes a valid consent, being that consent must be freely given, specific, informed and be one which is unambiguous.[465] An affirmative manner or an active act is required of the data subject prior to processing to constitute consent and this would effectively rule out any act of silence, pre-ticked boxes or inactivity of data subject.[466] Invalidation of consent can occur if there is economic imbalance between the controller and data subject.[467] Data subject is entitled

[457] GDPR, art 49(5).
[458] GDPR, art 49(1); GDPR, art 49(2); GDPR, recital 111.
[459] European Data Protection Board, 'Guidelines 2/2018 on derogations of Article 49' (n 455) 4.
[460] GDPR, recital of art 49(1).
[461] GDPR, art 48; European Data Protection Board, 'Guidelines 2/2018 on derogations of Article 49' (n 455) 5.
[462] GDPR, art 49(1).
[463] GDPR, art 49(2).
[464] GDPR, art 49(3).
[465] GDPR, art 4(11); GDPR, art 7; GDPR, art 8.
[466] GDPR, art 7; GDPR, recital 32; Elisabeth Meddin (n 148) 1003.
[467] GDPR, recital 43.

to withdraw from the consent given earlier and the effect of such withdrawal only affects future processing and does not have any retrospective effect in the aspect of lawfulness.[468] Where the right to withdraw consent has been withheld and the data subject does not have any freedom to do so without any detriment, this would vitiate the concept of 'freely given'.[469]

The threshold for consent is higher in CBPDT. For instance, specific consent must be obtained from data subject prior to any CBPDT despite personal data was already collected earlier.[470] To put differently, this applies to controller and/or processor with existing database of the personal data and the requirement of specific consent is crucial to data subject to meet the transparency requirements. The EDPB opined that it is impractical to request specific consent for future transfers in absence of specific details of the CBPDT as it hinders the impact assessment to be done effectually.[471] Additionally, data subject must be apprised of the specificities of data that will be transferred, the risks involved in that context, particularly where there is no adequate protection, to allow data subject to be informed and assess such circumstances.[472] The EDPB views that the high threshold of consent coupled with the right to withdraw consent may not be a sustainable solution for CBPDT.[473]

To date, it may still be that consent is a common ground for processing personal data especially in the commercial context.[474] Bergerman in his paper demonstrated the line of academic commentaries on the role of consent and accompanying criticism.[475] Axel Voss, a member of the European Parliament, opines that consent gives data users the 'illusion of control', however this can be disguised as a means for controllers to shift their responsibilities to data users.[476] It is easily observed that consent may easily be vitiated as a legitimate processing ground, particularly in the online context as data subject may just consent by ticking a box without reading or comprehending the privacy statement.[477] In a similar vein, an academician regards consent as a 'god-sent solution' given that most data subjects are complacent with signing away their agreement, particularly through online platforms, with enthusiasm to complete the

[468] GDPR, art 7.
[469] GDPR, recital 42.
[470] European Data Protection Board, 'Guidelines 2/2018 on derogations of Article 49' (n 455) 7.
[471] ibid.
[472] ibid, 5-7.
[473] ibid, 8.
[474] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250, 253.
[475] Benjamin Bergemann (n 449) 111 – 131.
[476] Axel Voss (n 151) 7.
[477] Koops (n 474) 253.

transaction at hand without first reading.[478] Goods or service providers may leverage on this weakness as consent is a 'key instrument for consumers to exchange their data in order to benefit from the services provided by internet companies'.[479] Other academicians viewed that the 'absence of meaningful choice' and overload of consent and information had led to the issue of 'consent desensitisation' which prevents consumers from making informed choices.[480] More so, with explicit consent which eventually led consumers to give away their consent blindly thus diminishing the value of consent and undermine data protection in the long run.[481] The author submits that these challenges raised by academicians may be mitigated with the transparency principle under GDPR which requires the information to be presented in plain language, succinct, intelligible and concise manner.[482] It established that derogations by way of consent must be restricted to specific circumstances and frequencies. Additionally, assessment shall be carried out by the controller and/or processor on the circumstances of data transfer and implement appropriate safeguards besides informing the supervisory authorities of the international data transfer.[483]

6.1 Redefining the Concept of Consent

It is observed that there is a stark contrast evidently seen in the use of explicit consent, based on an overall assessment of the PDPA which firstly lack the definition of consent and absence of limitations on the utilisation of CBPDT premised on consent. The disparity constitutes a defect which may be damaging in the long run, as the current framework of the PDPA seems to place huge reliance on the elements of explicit consent and necessary processing for CBPDT. The author submits that amendment should be made to the PDPA to draw the necessary parameters to the use of consent in the aspect of CBPDT which should include defining the concept of consent as well as outlining specific circumstances in which a data user can rely on the explicit consent of data subjects for international transfer. The author finds that the PDPA could benefit from the GDPR in its employment of appropriate safeguards measures, one of which is to restrict the frequency of transferring of personal data on that ground and therefore enhance the transparency principle.

---

[478] Chris KH Kwan, 'Data Privacy for Lawyers: An Introduction' [2020] 1 Legal Network Series (A) cxxxi, 8.
[479] Benjamin Bergemann (n 449) 112.
[480] Bart Schermer, Bart Custers and Simone van der Hof, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16 Ethics and Information Technology, 171 – 182.
[481] Benjamin Bergemann (n 449) 116; Schermer, Custers and Hof (n 480) 171 – 182.
[482] GDPR, art 12; GDPR, recital 39; Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 212).
[483] GDPR, recital of art 49(1).

[H] Chapter 7: Juxtaposition of the PDPA vs the GDPR

7.1 Parallel Principles of the PDPA and the GDPR

In the previous chapters, this paper set out the position of both frameworks on the PDP principles, legal entitlements, approach towards CBPDT including the diversity of mechanisms used. For this chapter, the author will examine the areas of law where the PDPA and the GDPR converge.

7.1.1 Equivalent Data Protection Principles

The concepts of PDP in both jurisdictions share fundamental similarities albeit with differences in the extent of their PDP measures. Perhaps the reason is because the PDPA was inspired by the Directive whilst the GDPR is a version built on its predecessor, the Directive.[484] Despite having different legal terminology, each jurisdiction shares basic PDP principles such as lawful processing grounds, transparency, purpose limitation, security principles, data minimisation, accuracy and accountability.[485] The use of general principles under the PDPA is the same as the 'lawfulness, fairness and transparency' principle which prescribes the legitimate grounds for processing.[486] The notice and choice principle under the PDPA shares similar elements as the purpose limitation of the GDPR.[487] Such principles are necessary to ensure data subject is fully informed of the processing activities prior to the collection of the personal data allowing the data subject options on whether to consent to the processing of their personal data.[488]

The disclosure principle enumerated in the PDPA permits disclosure of personal data in situations where consent has been obtained or where it is necessary for processing to take place, and this reflects that of the data minimisation principle under the GDPR.[489] Although the PDPA and the GDPR converge in PDP principles as such, the author observes that the GDPR provides a detailed guidance on the enforcement of mandatory security measures as well as measures to enhance security such as pseudonymisation and encryption.[490] Both the frameworks recognise data retention principle.[491] The PDPA places the onus on the data user to take reasonable efforts

---

[484] Pillai and Yong (n 24) 293.
[485] GDPR, art 5; GDPR, art 6; PDPA, section 5; PDPA, section 6.
[486] PDPA, section 5; GDPR, art 6.
[487] PDPA, section 7; GDPR, art 5(1)(b).
[488] Tobias Naef, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU law and International Trade Law'* (1st edn, Springer 2023) <https://doi.org/10.1007/978-3-031-19893-9> accessed 15 August 2023.
[489] PDPA, section 8; PDPA, section 39; GDPR, art 5(1)(d).
[490] GDPR, art 32(1).
[491] PDPA, section 10; GDPR, art 5(1)(e).

to ensure all the data subject's personal data are destroyed or permanently deleted.[492] The GDPR takes a step further to provide alternative options in cases where personal data collected could either be deleted or anonymised to prevent any linkage or identification to the data subject.[493] This also applies to personal data that are no longer necessary for the original purpose for which it was collected.[494] There is an overlap in the data integrity and access principle under the PDPA and where the GDPR shares striking resemblance.[495]

The author submits that despite the two data protection legislations being derived from the parent legislation which is the Directive, the GDPR stands out as a more inventive development with well-thought-out scope of protection to tackle the challenges in digital domain.[496] Additionally, the author submits that the impediments of the PDPA, to be elaborated later, could potentially undermine the current existing trade connections between Malaysia and the EU. As a result of the comparison between the frameworks, there are several aspects of the PDPA which necessitates review and modifications, however, the author proposes to discuss the key areas of the PDPA which lacks effectiveness.

7.2 Impediments of the PDPA in comparison to the GDPR

7.2.1 Public Sectors Exempted from the Application of PDPA

The application of the PDPA is confined specifically to commercial transactions.[497] It further applies to personal data outside Malaysia which are intended to be further processed in Malaysia.[498] Public sectors are excluded from its scope, and this is contrary to the EU legal framework which extends its coverage of GDPR to public authorities via the Law Enforcement Directive[499].[500]

The exclusion of government authorities from the application of the PDPA garnered criticism as academicians viewed this as an impartial approach which raises an inquiry about the varying

[492] PDPA, section 10; GDPR, art 5(1)(e).
[493] ibid.
[494] ibid.
[495] PDPA, section 12; GDPR, art 5(1)(d).
[496] Federal Legislation, 'Act 709 Personal Data Protection Act 2010' (*Federal Legislation Portal*) <https://lom.agc.gov.my/act-detail.php?act=709&lang=BI&date=15-06-2016#timeline> accessed 15 August 2023.
[497] PDPA, section 3(1).
[498] PDPA, section 3(2).
[499] LED.
[500] PDPA, section 3(1); LED.

criteria that regulate public and private entities.[501] The author views that such exclusion is unappealing to international businesses and could constitute trade barrier as there is no legal framework in place to hold the public authorities accountable. After all, government authorities have unrestricted access to personal data of nationals and foreigners.[502] Over the past years, there have been several news pertaining to data leakage which purportedly stems from public authorities.[503] The affected data subjects have no recourse in holding any organisation, body, or authority accountable for damage done. Therefore, the author opines that the absence of reparation has severe consequences and potentially creates an obstacle to trade and may render efforts to attract international businesses futile given the lack of protection over the processing of personal data of foreign nationals.

With the progression of technology and the integration of personal data into digital trade of goods and services, there is an increasing demand and importance for there to be a constant data flow to keep businesses going.[504] As the EU recognises PDP as a fundamental right under the Charter, there is also an increased awareness in individuals of their data rights. Likely, this approach may steer businesses or in fact countries who wish to be trading partners of EU to comply with data protection laws to carry out trading activities. Ever since the GDPR came into operation, countries in other jurisdiction have followed the footsteps of EU to implement GDPR-like legislation such as Thailand.[505] The author submits that the Malaysian policymakers may consider lifting the exemption of the PDPA on public authorities to strengthen the data protection framework.

7.2.2 Inadequacy of Mechanisms for Cross-Border Personal Data Transfer

In a previous chapter, this paper examined the various mechanisms of CBPDT. They are the adequacy decision, appropriate safeguards, and derogations in exceptional circumstances.[506] Comparatively, the PDPA recognises the adequacy and derogation. Although the PDPA also recognises certain transfer tools under the GDPR, they are not effectively implemented in

[501] Yusof (n 24) 132.
[502] Kwan (n 478) 1.
[503] BBC (n 51); Rahimi Yunus (n 51); Aaron Raj (n 51); The Vibes, 'Hackers claim to have personal details of 22.5 mil Malaysians' (*The Vibes,* 18 May 2022) https://www.thevibes.com/articles/news/61117/hacker-group-claims-to-have-personal-details-of-22.5-mil-malaysians accessed 15 August 2023.
[504] Yakovleva (n 13) 883.
[505] Gstrein and Zwitter (n 61); Graham Greenleaf, 'Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock' (2019) No 4, Revista Uruguaya de Protección de Datos Personales (Revista PDP), August 2019, 49, 52 <https://ssrn.com/abstract=3483794> accessed 15 August 2023.
[506] GDPR, chapter V.

practice. There is implementation of the PDPA-COP, which is being used, however, it shall be read together with the PDPA, which has limited and inadequate CBPDT provisions.[507] The author submits that firstly, there is inadequacy of the CBPDT to permit international transfer and could benefit from the various tools under appropriate safeguard.[508] Secondly, the mechanisms readily available in the PDPA are not effectively implemented in practice, hence the author submits this as a deficiency. One of the reasons for this is that the PDPA Whitelist Order did not materialise.[509] In respect of the proposed blacklist approach, the author opines that the implementation of blacklist approach is not recommended as this is an easy approach of assuming that all third country jurisdictions have an adequate level of protection or substantially similar legislation as per the PDPA. The author views that the whitelist approach would be a secure and cautious approach, to an extent reflected by the adequacy decision in the GDPR, whereby assessment of the third country would have to be done prior to allowing any CBPDT.[510] In absence of any mechanisms to evaluate the third countries when considering the CBPDT, the author views the repercussions on the data subject may be manifold if there are any misuse, unauthorised or unlawful use of the personal data.

It appears that since there is no whitelist in force under the PDPA at this juncture, hence the only avenue available for data users to engage in CBPDT is by way of derogations, which can either be through explicit consent of data subject or where processing are necessary on statutory grounds.[511] Bearing in mind the criticisms of consent and consumers' behaviour towards it observed in ***Chapter 6*** and in absence of the definition of consent under the PDPA, the author views that the CBPDT premised on explicit consent alone is rather alarming.

7.2.3 Ill-equipped Data Protection Rights for Data Subjects in Digital Commerce Transactions

The assessment reveals that the PDPA is lacking in the right to erasure, data portability right and the right not to be subjected to automated decision-making and profiling. These shortfalls save and except the right to erasure are acknowledged by the PDPA Department in their public

[507] PDPA, section 129(1); Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Malaysia Aviation Sector'(n 429) 52-53; Department of Personal Data Protection, 'Personal Data Protection Code of Practice for the Banking and Financial Sector' (n 42) 46-47.
[508] GDPR, art 46.
[509] Baker McKenzie, 'International Data Transfer' (n 101).
[510] GDPR, art 45.
[511] PDPA, section 129(3).

consultation.[512] The author submits that the right to erasure, if adopted in the PDPA, is closely associated to the purpose limitation and retention principle. At the very least, the PDPA Standards and PDPA-COP has provided practical steps towards ensuring that inactive or unnecessary personal data are disposed of within stipulated time frame.[513] The additional rights portrayed in the GDPR which are unavailable under the PDPA such as the right to portability and right not to be subjected to automated decision-making and profiling are essential in the digital age and beneficial in according data subjects the right to control over their data in a more effective way.[514]

7.2.4 Absence of Autonomy of the PDPA-Commissioner

The author submits that it is essential for there to be an independent supervisory authority for the observation and compliance of the data protection laws and regulations, as prescribed in the GDPR.[515] Indeed, this is a fundamental pre-requisites for the EC when considering whether a third country has adequate protection via its laws and regulations for CBPDT.[516] It is stipulated in the GDPR that the supervisory authority shall act with complete independence, free from any external influence, be given the prerogative to appoint its own staff and be provided the resources and means to do so.[517]

The appointment of the PDPA-Commissioner, which should be made available publicly, is determined by the PDPA-Ministry who has the power to issue directions to PDPA-Commissioner regarding its responsibilities.[518] Academicians opine that this constitutes a lack of independence as the decisions made by PDPA-Commissioner is heavily influenced or reliant on the PDPA-Ministry, hence raising doubts on the effectiveness of the PDPA.[519] The independence of the PDPA-Commissioner could also be vitiated due to the statutory requirement to provide financial documents to and as directed by the PDPA-Ministry.[520] To this

[512] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18) 4-12.
[513]PDPA Standards, chapter 6 of Part II; PDPA Standards; Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (n 40) 24.
[514] Article 29 Data Protection Working Party, 'Adequacy Referential' (n 141) ch 3.
[515] GDPR, art 51(1).
[516] GDPR, art 45(2).
[517] GDPR, art 52.
[518] PDPA, section 47(1); PDPA, section 47(2); PDPA, section 59(2).
[519] Md Toriqul Islam, Abu Bakar Munir & Mohammad Ershadul Karim, 'Revisiting the Right to Privacy in the Digital Age: A Quest to Strengthen the Malaysian Data Protection Regime' (2021) 48 Journal of Malaysian and Comparative Law 49, 67; Yusof (n 24) 128.
[520] PDPA, section 60(1); Islam, Munir & Karim, 'Revisiting the Right to Privacy in the Digital Age' (n 519) 67; Greenleaf, 'Asia's Data Privacy Dilemmas 2014–19: National Divergences' (n 505) 64.

end, the author adds that unless there are clear provisions in the PDPA to segregate and establish independence for the PDPA-Commissioner, the close interrelation between the PDPA-Commissioner and PDPA-Ministry may undermine the efficacy of the PDPA as a whole.

7.2.5 Unavailability of Direct Enforcement Mechanisms by individuals

Any contravention of the PDPA and/or its subsidiary legislation is subject to fine and/or imprisonment,[521] however, the prosecution of offences can only be pursued against the alleged offender provided the written consent of the public prosecutor is first obtained.[522] The only direct avenue provided for the individuals is the filing of a complaint for investigation of infringement of rights, however the ultimate decision for prosecution is in the hands of the public prosecutor.[523] The author submits that the PDPA ought to accord right to an effective remedy to data subjects, as seen in the GDPR, whereby data subjects are able to commence court actions against the supervisory authority or the controller and/or processor.[524] Absence of direct enforcement in place except for a civil suit by the data subject against the data user by way of common law,[525] weakens the efficiency of the PDPA. The author views that a proposed amendment to accord the data subject the direct enforcement mechanism would be in line with the accountability principle and ensure that the data user conform to the principles prescribed under the PDPA.

[521] PDPA, section 5(2); PDPA, section 42(6); PDPA, section 43(4).
[522] PDPA, section 134.
[523] PDPA, section 104.
[524] GDPR, art 78; GDPR, art 79.
[525] Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020' (n 18) 8; Baker McKenzie, 'Penalties for Non-Compliance' (n 324).

[I] CONCLUSION

This paper had evaluated the various CBPDT mechanisms under the GDPR and to consider the adoption of these mechanisms to the judicial landscape of Malaysia. To do so, this paper has undertaken a comprehensive comparative analysis of the PDPA and the GDPR extensively. The findings revealed a degree of similarity between the two frameworks to an extent pertaining to the fundamental principles of data protection and the legal entitlements granted to the data subject. This paper had earlier highlighted notable disparity between the PDPA and the GDPR, thus revealing impediments to the PDPA illustrated in ***Chapter 7.2***. Even with these distinctions, the author maintains the perspective that the PDPA does not diverge significantly from the GDPR, thus permitting the possibility for advancement by the policymakers in Malaysia to reinforce the PDP rights in Malaysia. Briefly, the author submits that some of the proposed areas for enhancement would entail expanding the applicability of the PDPA to include government authorities, broadening the rights accorded to data subjects to better address the digital requirements such as the right to erasure and pertaining to automated decision-making, strengthening the existing avenues of CBPDT on consent and adequacy mechanisms, adopt the appropriate safeguards of the GDPR, and introduce an effective direct enforcement mechanism.

It is observed that there are overlapping areas between two frameworks, and this resemblance could leverage the potential of Malaysia of being considered by the EU as having adequate protection level. After all, the EU-Malaysia had advanced as Trading Partners by virtue of the PCA. The policymakers of Malaysia recognised the pressing need to revise the PDPA, hence the author submits that the serious deficiencies of the PDPA in ***Chapter 7.2*** be rectified expeditiously to strengthen the PDP which consequentially enhance its appeal as a trading partner before commencing any negotiations to explore a potential adoption of adequacy. Ideally, Malaysia can attain the ‘adequacy’ status recognised by the EU. However, it is acknowledged that the adequacy process spans several years due to the audit and approval processes to be undertaken. Nevertheless, the author views that the doors for CBPDT is not completely shut pending the process or adoption of the assessment of adequacy.

As previously examined, there are a myriad of suitable safeguards introduced by the GDPR. Malaysia had through ASEAN adopted the use of MCC, which is the base framework to the SCC however, this is not implemented in practice. The author submits that the policymakers should enforce this by enactment in the PDPA or through subsidiary legislations to enforce the

application of MCC within the ASEAN region or to improvise it further to a level enumerated by the SCC. Alternatively, Malaysia may consider adopting the BCR which has a similar framework as the CBPR which Malaysia has indicated interest to adopt. The author submits that the adoption of BCR as a means of CBPDT would be a valuable addition which could be enacted in the company legislation, Malaysian Companies Act 2016 to enforce uniformly across all the corporations in Malaysia involved in CBPDT. In fact, this could be applied to domestic PDT as well. Akin to the GDPR, Malaysia had implemented the use of PDPA-COP, which has a parallel role to the COC. Although the implementation of the PDPA-COP is useful, it appears to have been underutilised as the principles therein aligned with the PDPA, hence, the author submits that where suggested amendments are made to the PDPA, this would consequentially add value to the use of PDPA-COP. In respect of the certification mechanism, the author views that this may not be feasible for Malaysia, as the process for the certification takes a long time, and by far, there have only been one EU country which has obtained the certification, which is Luxembourg.[526] This paper earlier proposed to extend the application of the PDPA to bind public authorities as this would promote accountability on their end as well as to improve the appeal for CBPDT with governmental bodies of third countries. In this regard, the author views that it would be best to consider this at a later stage as this transfer mechanism would be premised on international treaties to safeguard the free movement of personal data and at present, the public authorities in Malaysia remains excluded from the application of the PDPA.

As for CBPDT by way of derogation, the author submits there is a pressing need to conceptualise the definition of consent and explicit consent as there is ambiguity attached to it and may be challenging to establish a processing based on consent as legitimate. Indeed, the proposal to introduce would be a significant enhancement as it elucidates what constitutes consent. Additionally, the PDPA could emulate the GDPR in the limitations attached to the use of CBPDT by way of derogation, i.e., restricting the use to a non-repetitive processing task and requiring the data exporter to ensure that appropriate safeguards are in place prior to the transfer. The author concludes that in consideration of the PCA entered by the Trading Partners and corresponding to Malaysia's vision to accelerate digital trade and economy, it is an opportune time for the policymakers to revisit the PDPA and consider emulation of the GDPR to an extent deemed appropriate.

[526] European Data Protection Board, 'The CNPD adopts the certification mechanism GDPR-CARPA' (n 411).

BIBLIOGRAPHY

I. PRIMARY SOURCES

A. EU Legislations / Regulations

1. Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
2. Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/1.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31.
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119/89.

B. Malaysian Legislations / Regulations

1. Personal Data Protection 2010 (Act 709) (Malaysia).
2. Personal Data Protection Regulations 2013 PU (A) 335/2013.
3. Personal Data Protection (Class of Data Users) Order 2013 PU (A) 336/2013.
4. Personal Data Protection (Registration of Data User) Regulations 2013 PU (A) 337/2013.
5. Personal Data Protection (Class of Data Users) (Amendment) Order 2016 PU (A) 326/2016.
6. Personal Data Protection Standards 2015.

C. International Treaty/Conventions

1. European Parliament non-legislative resolution of 14 June 2023 on the draft Council decision on the conclusion, on behalf of the Union, of the Framework Agreement on Partnership and Cooperation between the European Union and its Member States, of the one part, and the Government of Malaysia, of the other part (11714/2022 – C9-0430/2022 – 2022/0221M(NLE)) < https://www.europarl.europa.eu/doceo/document/TA-9-2023-0234_EN.html> accessed 15 August 2023.
2. Framework Agreement on Partnership and Cooperation between the European Union and its member states, of the one part, and the Government of Malaysia, of the other part 11732/22 (Brussels, 3 October 2022) <https://data.consilium.europa.eu/doc/document/ST-11732-2022-INIT/en/pdf> accessed 15 August 2023.

D. EU case laws

1. Joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen* [2010] ECR I-11063.
2. Case C-291/12 *Michael Schwarz v Stadt Bochum* (GC, 17 October 2013).
3. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (GC, 8 April 2014).
4. Case C-362/14 Maximillian Schrems v Data Protection Commissioner (GC, 6 October 2015] ("Schrems I").
5. Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (GC, 16 July 2020) ("Schrems II").
6. Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (GC, 16 July 2020), Opinion of AG Saugmandsgaard Øe.

II. SECONDARY SOURCES

A. Books

1. Directorate-General for Communication (European Commission), *The European Union: What it is and what it does* (Publications Office of the European Union 2022).
2. Kosta E, Lees R, Kamara I (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar 2022).
3. Kuner C, Bygrave L A, Docksey C and Drechsler L (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).
4. Kuner C and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary – Update of Selected Article* (Oxford University Press 2021).
5. Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
6. Pillai D and Yong SH, 'The Privacy, Data Protection and Cybersecurity Law Review: Malaysia' in Raul AC (9th edn), *The Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd 2022).
7. Walters R, Trakman L and Zeller B, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (Springer 2019).

B. Contribution to Edited Books

1. Bergemann B, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection' in Hansen M and others (eds), *Privacy and Identity Management: The Smart Revolution* (Springer 2018).
2. Greenleaf G, 'Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains' in Svantesson DJB and Kloza D (eds), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy (Intersentia 2018).
3. Munir AB, 'Malaysia's Data Protection Law' in Chesterman S (ed), *Data Protection Law in Singapore* (Academy Publishing 2014).
4. Roessler B, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy' in Roessler B and Mokrosinska D (eds), *Social Dimensions of Privacy: Interdisciplinary Perspective* (Cambridge University Press, Cambridge 2015).
5. Tzanou M, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Fabbrini F, Celeste E and Quinn J (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Bloomsbury 2021).

C. Journal Articles

1. Brkan M, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23(5) Maastricht Journal of European and Comparative Law 812.
2. Burri M and Schär R, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 Journal of Information Policy 479.
3. Greenleaf G, 'ASEAN data privacy developments 2014-15' (2015) 134 Privacy Laws & Business International Report 9.
4. Islam MT and Karim ME, 'Extraterritorial Application of The Eu General Data Protection Regulation: An International Law Perspective' (2020) 28(2) IIUM Law Journal 531.
5. Koops BJ, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250.
6. Kwan CKH, 'Data Privacy for Lawyers: An Introduction' [2020] 1 Legal Network Series (A) cxxxi.
7. Meddin E, 'The Cost of Ensuring Privacy: How The General Data Protection Regulation Acts as a Barrier To Trade In Violation Of Articles XVI And XVII Of The General Agreement On Trade In Services' (2020) 35(4) American University International Law Review 997.
8. Sureani NBN and others, 'The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia' (2021) 6 Malaysian Journal of Social Sciences and Humanities 488.
9. Schermer B, Custers B and Hof SVD, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16 Ethics and Information Technology, 171.
10. Yakovleva S, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities' (2020) 21 Journal of World Investment & Trade 881.
11. Yakovleva S and Irion K, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade' (2020) 10 International Data Privacy Law 201.
12. Yusof ZM, 'The Malaysian Personal Data Protection Act 2010: A Legislation Note' (2011) 9 New Zealand Journal of Public and International Law 119.

D. Online Publication

1. Chan M, 'Digital Payments, Data Regulations, and AI as Most Promising Areas for Digital Economy Collaboration' in Paul Cheung and Xie Taojun (eds), *The ASEAN Digital Economy: Towards an Integrated Regional Framework* (Routledge 2024) <https://books.google.ie/books?hl=en&lr=&id=XEDJEAAAQBAJ&oi=fnd&pg=PA76&ots=C_aOf38yUH&sig=dho0sXRnLVgNVmvGk9KM6z39NKw&redir_esc=y#v=onepage&q&f=false> accessed 15 August 2023.
2. Callo-Müller MV, 'GDPR and CBPR: Reconciling Personal Data Protection and Trade' (2018) APEC Policy Support Unit POLICY BRIEF No. 23 <https://www.apec.org/docs/default-source/Publications/2018/10/GDPR-and-CBPR---Reconciling-Personal-Data-Protection-and-Trade/218_PSU_Policy-Brief_GDPR_CBPR.pdf> accessed 15 August 2023.
3. Costello RA, 'Schrems II: Everything Is Illuminated?' (2020) 5 European Papers 703, 1053 <https://www.europeanpapers.eu/sites/default/files/EP_eJ_2020_2.pdf> accessed 15 August 2023.
4. Greenleaf G, 'Malaysia: ASEAN's first data privacy Act in force' (2013) University of New South Wales Law Research Paper No. 12/2014, 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2404893> accessed 15 August 2023.
5. Greenleaf G, 'ASEAN data privacy developments 2014-15' (2015) 134 Privacy Laws & Business International Report, UNSW Law Research Paper No. 2015-48 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2645702#> accessed 15 August 2023.
6. Greenleaf G, Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock (2019) No 4, Revista Uruguaya de Protección de Datos Personales (Revista PDP), August 2019, 49, 52 <https://ssrn.com/abstract=3483794> accessed 15 August 2023.
7. Maria T, Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights (October 13, 2020). Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, Forthcoming, Available at SSRN: <https://ssrn.com/abstract=3710539> accessed 15 August 2023.
8. Naef T, *Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU law and International Trade Law'* (1st edn, Springer 2023) <https://doi.org/10.1007/978-3-031-19893-9> accessed 15 August 2023.

9. Velli F, 'The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements' (2019) 4(3) European Papers 881, 881 <https://doi.org/10.15166/2499-8249/325> accessed 15 August 2023.
10. Wahl T, 'Commission Adopted Adequacy Decision for South Korea' (EUCRIM, 22 December 2021) <https://eucrim.eu/news/commission-adopted-adequacy-decision-for-south-korea/> accessed 15 August 2023.

E. European Data Protection Board / Article 29 Working Party Publications

1. Article 29 Working Party, 'Guidelines on the right to data portability' (European Commission, 5 April 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> accessed 15 August 2023.
2. Article 29 Data Protection Working Party, 'Adequacy Referential' (*European Commission*, 6 February 2018) WP 254 rev 01 <https://ec.europa.eu/newsroom/article29/items/614108> accessed 15 August 2023.
3. Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR (European Commission, 11 April 2018) <https://commission.europa.eu/document/download/dec4329d-951e-41e2-82e9-b0ade63c0d8b_en> accessed 15 August 2023.
4. Article 29 Data Protection Working Party, 'Guidelines on transparency under Regulation 2016/679' (*Article 29 Data Protection Working Party*, 11 April 2018) WP260 rev 01 <https://ec.europa.eu/newsroom/article29/items/622227/en> accessed 15 August 2023.
5. European Data Protection Board, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' (European Data Protection Board, 25 May 2018) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf> accessed 15 August 2023.
6. European Data Protection Board, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (European Data protection Board, 22 February 2022) <https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf> accessed 15 August 2023.
7. European Data Protection Board, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' (*European Data Protection Board*, 7 January 2020)

<https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_0.pdf> accessed 15 August 2023.

8. European Data Protection Board, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR' (*European Data Protection Board*, 14 February 2023) <https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf> accessed 15 August 2023.
9. EDPB, 'Guidelines 07/2022 on certification as a tool for transfers' (*EDPB*, 14 February 2023) <https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf> accessed 15 August 2023.
10. European Data Protection Board, 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies' (European Data Protection Board, 15 December 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf> accessed 15 August 2023.
11. European Data Protection Board, 'Guidelines 04/2021 on Codes of Conduct as tools for transfers' (European Data protection Board, 22 February 2022), <https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf> accessed 15 August 2023.

F. Official Publications by EU bodies

1. Council of the EU, 'Indo-Pacific: The European Union and Malaysia sign Partnership and Cooperation Agreement' (*European Council*, 14 December 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/14/indo-pacific-the-european-union-and-malaysia-sign-partnership-and-cooperation-agreement/#:~:text=The%20Partnership%20and%20Cooperation%20Agreement,that%20started%20in%20October%202010> accessed 15 August 2023.
2. Data Protection Commissioner of Ireland, 'Transfers of Personal Data to Third Countries or International Organisations' (*Data Protection Commissioner*) <https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations> accessed 15 August 2023.

3. Directorate-General for Justice and Consumers, 'The New Standard Contractual Clauses – Questions and Answers' (*European Commission*, 4 June 2021), 4 <https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf> accessed 15 August 2023.
4. Directorate-General for Justice and Consumers, 'Standard contractual clauses for international transfers' (*European Commission,* 4 June 2021) <https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en> accessed 15 August 2023.
5. Directorate-General for Justice and Consumers, 'Standard contractual clauses for controllers and processors in the EU/EEA' (*European Commission*, 4 June 2021) <https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en> accessed 15 August 2023.
6. Directorate-General for Justice and Consumers, 'Joint Guide to ASEAN Model Contractual Clauses and EU Standard Clauses' (*European Commission*, 24 May 2023) <https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf> accessed 15 August 2023.
7. European External Action Service Press Team Press Team, 'EU-Malaysia Relations' (*European Union External Action*, 13 January 2023) <https://www.eeas.europa.eu/sites/default/files/documents/EU-Malaysia%20factsheet.pdf> accessed 15 August 2023.
8. European Data Protection Board, 'The CNPD adopts the certification mechanism GDPR-CARPA' (*EDPB*, 27 June 2022) <https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en> accessed 15 August 2023.
9. European Data Protection Supervisor, 'The History of the General Data Protection Regulation' (*European Data Protection Supervisor*) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,as%20law%20across%20the%20EU> accessed 15 August 2023.
10. European Data Protection Supervisor, 'The History of the General Data Protection Regulation' (*European Data Protection Supervisor*) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 15 August 2023.

11. European Free Trade Association, 'General Data Protection Regulation incorporated into the EEA Agreement' (*European Free Trade Association*, 6 July 2018) <https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291> accessed 15 August 2023.
12. European Free Trade Association, 'Data Protection' (*European Free Trade Association*) <https://www.efta.int/EEA/Data-Protection-505036> accessed 15 August 2023.
13. European Parliament, 'EU-Malaysia Partnership and Cooperation Agreement' (*Legislative Observatory European Parliament*, 14 June 2023) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1747973&t=d&l=en> accessed 15 August 2023.
14. European Union, 'Implementing Acts' (*EUR-Lex*) <https://eur-lex.europa.eu/EN/legal-content/glossary/implementing-acts.html#:~:text=These%20acts%20aim%20to%20create,have%20individual%20or%20general%20applications.> accessed 15 August 2023.

G. Official Publications of Malaysian Government Bodies

1. Attorney General's Chambers of Malaysia, 'Personal Data Protection Act 2010' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-detail.php?act=709&lang=BI&date=15-06-2016#timeline> accessed 15 August 2023.
2. Attorney General's Chambers of Malaysia, 'Personal Data Protection Regulations 2013' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20335/2013> accessed 15 August 2023.
3. Attorney General's Chambers of Malaysia, 'Personal Data Protection (Registration of Data User) Regulations 2013' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20337/2013> accessed 15 August 2023.
4. Attorney General's Chambers of Malaysia, 'Appointment of Date Coming into Operation' (*Federal Legislation Portal of Malaysia)* <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(B)%20464/2013> accessed 15 August 2023.
5. Attorney General's Chambers of Malaysia, 'Personal Data Protection (Class of Data Users) Order 2013' (*Federal Legislation Portal of Malaysia*) <https://lom.agc.gov.my/act-view.php?type=pua&no=P.U.%20(A)%20336/2013> accessed 15 August 2023.

6. Department of Personal Data Protection, 'Public Consultation Paper No. 01/2020 Review of Personal Data Protection Act 2010 (Act 709)' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf> accessed 15 August 2023.
7. Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (*Official Portal of Department of Personal Data Protection*, 15 December 2022) 5 <https://www.pdp.gov.my/jpdpv2/assets/2023/01/28.12.2022-FINAL-PRINTING-COP-BI.pdf> accessed 15 August 2023.
8. Department of Personal Data Protection, 'Introduction' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/about-us/organization-profile/introduction/?lang=en> accessed 15 August 2023.
9. Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Malaysia Aviation Sector' (*Official Portal of Department of Personal Data Protection*, 21 November 2017) <https://www.pdp.gov.my/jpdpv2/tata_amalan/the-personal-data-protection-code-of-practice-for-the-malaysia-aviation-sector/> accessed 15 August 2023.
10. Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for the Utilities Sector (Electricity' (*Official Portal of Department of Personal Data Protection*, 23 June 2016) <https://www.pdp.gov.my/jpdpv2/tata_amalan/the-personal-data-protection-code-of-practice-for-the-utilities-sector-electricity/> accessed 15 August 2023
11. Department of Personal Data Protection, 'Personal Data Protection Code of Practice for the Banking and Financial Sector' (*Official Portal of Department of Personal Data Protection*, 19 January 2017) <https://www.pdp.gov.my/jpdpv2/tata_amalan/personal-data-protection-code-of-practice-for-the-banking-and-financial-sector/> accessed 15 August 2023.
12. Department of Personal Data Protection, 'Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia' (*Official Portal of Department of Personal Data Protection*, 23 December 2016) <https://www.pdp.gov.my/jpdpv2/tata_amalan/code-of-practice-on-personal-data-protection-for-the-insurance-and-takaful-industry-in-malaysia/> accessed 15 August 2023.
13. Department of Personal Data Protection, 'The Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry' (*Official Portal of Department of*

Personal Data Protection) <https://www.pdp.gov.my/jpdpv2/tata_amalan/the-personal-data-protection-code-of-practice-for-private-hospital-eng/> accessed 15 August 2023.

14. Department of Personal Data Protection, 'General Code of Practice of Personal Data Protection' (*Official Portal of Department of Personal Data Protection*, 15 December 2022) 5 <https://www.pdp.gov.my/jpdpv2/assets/2023/01/28.12.2022-FINAL-PRINTING-COP-BI.pdf> accessed 15 August 2023.
15. Department of Personal Data Protection, 'Tata Amalan *(Code of Practice)*' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/tata_amalan/> accessed 15 August 2023.
16. Department of Personal Data Protection, 'Personal Data Protection Standards 2015' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/assets/2019/09/BukuStandardPDP-2015.pdf> accessed 15 August 2023.
17. Department of Personal Data Protection, 'Asean Data Management Framework (Dmf) And Asean Model Contractual Clauses For Cross Border Data Flows (MCCs)' (*Official Portal of Department of Personal Data Protection*) <https://www.pdp.gov.my/jpdpv2/assets/2021/11/Guidelines-for-DMF-and-MCC-ASEAN.pdf> accessed 15 August 2023.
18. Economic Planning Unit, Prime Minister's Department, 'Malaysia Digital Economy Blueprint' (Government of Malaysia, February 2021) <https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf#page=55> accessed 15 August 2023.
19. Ministry of Foreign Affairs Malaysia, 'Malaysia and the European Union Inked the Partnership and Cooperation Agreement 14 December 2022, Brussels, Belgium' (*Ministry of Foreign Affairs Malaysia*, 15 December 2022) <https://www.kln.gov.my/web/guest/-/malaysia-and-the-european-union-inked-the-partnership-and-cooperation-agreement-14-december-2022-brussels-belgium> accessed 15 August 2023.
20. Ministry of Communications and Digital, 'Department and Agency Directory' (*Official Portal of Ministry of Communications and Digital*) <https://www.kkd.gov.my/en/directory-and-contact-us/direktori-jabatan-agensi> accessed 15 August 2023.

21. The Government of Malaysia, 'Personal Data Protection Act' (*The Government of Malaysia Official Gateway*) <https://www.malaysia.gov.my/portal/content/654> accessed 15 August 2023.

H. EU Commission Documents

1. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce OJ L 215/7.
2. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield OJ L 207/1.
3. European Commission, 'Communication from The Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 final.
4. European Commission, 'Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation COM (2020) 264 final.
5. Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance) OJ L 199/18.
6. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance) OJ L 199/31.
7. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council' COM (2023) 348 final.
8. European Commission, 'European Commission adopts new tools for safe exchanges of personal data' (*European Commission*, 4 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847> 15 August 2023.

9. European Commission, 'Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework' C(2023) 4745 final <https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf> accessed 15 August 2023.
10. European Commission, 'Data Protection in the EU' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> accessed 15 August 2023.
11. European Commission, 'Data Protection in the EU' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en> accessed 15 August 2023.
12. European Commission, 'Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation' (*European Commission*) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en> accessed 15 August 2023.
13. European Commission, 'Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows' (*European Commission*, 10 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721> accessed 15 August 2023.
14. European Commission, 'Adequacy Decisions' (*European Commission*) <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 15 August 2023.
15. European Commission, 'Malaysia: EU Trade relations with Malaysia. Facts, figures and latest developments' (*European Commission*) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/malaysia_en> accessed 15 August 2023.

I. Working Papers

1. Drechsler L, 'What Is Equivalent? A Probe into GDPR Adequacy Based on EU Fundamental Rights' (2019) Jusletter IT <https://ssrn.com/abstract=3549252> accessed 15 August 2023.
2. Kuner C, 'Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection' (2021) University of Cambridge Faculty of Law Research Paper No. 20/2021, 15 <https://ssrn.com/abstract=3827850> accessed 15 August 2023.
3. Graham G, Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains (2016) in Dan Svantesson and Dariusz Kloza 'Transatlantic Data Privacy Relationships as a Challenge for Democracy' (European Integration and Democracy series) (Intersentia, 2017), UNSW Law Research Paper No. 2016-08, 3 <https://ssrn.com/abstract=2732386> or <http://dx.doi.org/10.2139/ssrn.2732386> accessed 15 August 2023.
4. Greenleaf G, 'ASEAN Model Contractual Clauses: low and ambiguous data privacy standards' (2021) 174 *Privacy Laws & Business International Report* 22-24, UNSW Law Research Paper No. 21-83, 1 <http://www8.austlii.edu.au/cgi-bin/viewdoc/au/journals/UNSWLRS/2021/83.html> accessed 15 August 2023.
5. Gstrein OJ and Zwitter AJ, 'Extraterritorial application of the GDPR: promoting European values or power?' (2021) 10(3) Internet Policy Review 1, <https://doi.org/10.14763/2021.3.1576> accessed 15 August 2023.

J. Newspaper articles

1. BBC, 'Malaysian data breach sees 46 million phone numbers leaked' (*BBC*, 31 October 2017) <https://www.bbc.com/news/technology-41816953> accessed 15 August 2023.
2. Bernama, 'Fahmi: Personal data protection act needs amending to avoid data abuse' (New Straits Times, 18 June 2023) <https://www.nst.com.my/news/nation/2023/06/921606/fahmi-personal-data-protection-act-needs-amending-avoid-data-abuse> accessed 15 August 2023.
3. Bernama, 'Saifuddin: Malaysia committed to helping Asean secure data flow, enhance cyber security' (*New Straits Times*, 21 January 2021)<https://www.nst.com.my/news/nation/2021/01/659340/saifuddin-malaysia-committed-helping-asean-secure-data-flow-enhance-cyber> accessed 15 August 2023.

4. Lim A, 'Capitalize on technology to strengthen your data security' (The Star, 23 June 2023) <https://www.thestar.com.my/business/business-news/2023/06/23/capitalise-on-technology-to-strengthen-data-security> accessed 15 August 2023.
5. MalayMail, 'Fahmi: Amendments to Personal Data Protection Act to be tabled in Parliament by year end', (The MalayMail, 25 January 2023) <https://www.malaymail.com/news/malaysia/2023/01/25/fahmi-amendments-to-personal-data-protection-act-to-be-tabled-in-parliament-by-year-end/51871> accessed 15 August 2023.
6. Yunus R, 'Almost 200% increase in data breach attacks since 2018' (*The Malaysian Reserve*, 17 October 2019) https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/ accessed 15 August 2023.
7. The Vibes, 'Hackers claim to have personal details of 22.5 mil Malaysians' (*The Vibes,* 18 May 2022) <https://www.thevibes.com/articles/news/61117/hacker-group-claims-to-have-personal-details-of-22.5-mil-malaysians> accessed 15 August 2023.

K. Websites

1. Asia-Pacific Economic Cooperation, 'Member Economies' (*Asia-Pacific Economic Cooperation*) <https://www.apec.org/About-Us/About-APEC/Member-Economies> accessed 15 August 2023.
2. ASEAN, 'ASEAN Model Contractual Clauses for Cross Border Data Flows' (ASEAN, January 2021) <https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf> accessed 15 August 2023.
3. ASEAN, 'ASEAN member states' (*Association of Southeast Asian Nationals*' <https://asean.org/member-states/> accessed 15 August 2023.
4. Bradford L, Aboy M and Liddel K, 'Standard contractual clauses for cross-border transfers of health' (2021) 8 Journal of Law and the Biosciences 1, 3 <https://academic.oup.com/jlb/article/8/1/lsab007/6306998> accessed 15 August 2023.
5. Centre for Information Policy Leadership, International Data Flows: Cross Border Privacy Rules, Privacy Recognition for Processors, and Global CBPR and PRP (*Centre for Information Policy Leadership*, July 2023) 5 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cbpr_prp_faq_updated_july23.pdf> accessed 15 August 2023.

6. Christopher & Lee Ong, 'Personal Data Protection Updates – Public Consultation Paper No. 1/2017 – Personal Data Protection (Transfer of Personal Data To Places Outside Malaysia) Order 2017' (*Rajah & Tann Asia*, April 2017) <https://www.christopherleeong.com/media/2785/personal-data-protection-transfer-of-personal-data-to-places-outside-malaysia-order-2017.pdf> accessed 15 August 2023.
7. Christopher & Lee Ong, 'Latest Update on the Proposed Amendments to the Personal Data Protection Act 2010' (*Christopher & Lee Ong*, August 2022) <https://www.christopherleeong.com/media/5004/2022-08_clo_pdpa-amendments-oct-2022.pdf> accessed 15 August 2023.
8. Cory N, Dick E and Castro D, 'The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade' (Information Technology & Innovation Foundation, 17 December 2020) <https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade/> accessed 15 August 2023.
9. Digital Watch, 'Revision of Malaysia's Personal Data Protection Act 2010 is needed, Minister of Communications and Digital Communications claims' (*Digital Watch*, 18 June 2023) <https://dig.watch/updates/revision-of-malaysias-personal-data-protection-act-2010-is-needed-minister-of-communications-and-digital-communications-claims> accessed 15 August 2023.
10. Freehills HS, 'Privacy law reform in Malaysia: One step closer to mandatory breach notification' (*Herbert Smith Freehills*, 17 August 2022) <https://hsfnotes.com/data/2022/08/17/privacy-law-reform-in-malaysia-one-step-closer-to-mandatory-breach-notification/> accessed 15 August 2023.
11. Hogan Lovells Publications, 'Malaysia Publishes draft "White List" for personal data exports' (*Hogan Lovells*, 27 April 2017) <https://www.hoganlovells.com/en/publications/malaysia-publishes-draft-white-list-for-personal-data-exports> accessed 15 August 2023.
12. McKenzie B, 'ASEAN: Adopting the ASEAN Model Contractual Clauses for cross-border data transfers' (*Baker McKenzie*, 2 November 2021) <https://insightplus.bakermckenzie.com/bm/data-technology/asean-adopting-the-asean-model-contractual-clauses-for-cross-border-data-transfers_1> accessed 15 August 2023.
13. McKenzie B, 'International Data Transfer' (*Baker McKenzie*, 30 December 2022) <https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/malaysia/topics/international-data-transfer> accessed 15 August 2023.

14. McKenzie B, 'Penalties for Non-Compliance' (Baker McKenzie, 30 December 2022) <https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/malaysia/topics/penalties-for-non-compliance> accessed 15 August 2023.
15. McKenzie B, 'Data Privacy and security' (Baker McKenzie) <https://resourcehub.bakermckenzie.com/en/resources/cloud-compliance-center/apac/malaysia/topics/data-privacy-and-security> accessed 15 August 2023.
16. Medina AF, 'The European Union and Malaysia Sign Partnership and Cooperation Agreement' (*Asean Briefing*, 30 January 2023) <https://www.aseanbriefing.com/news/the-european-union-and-malaysia-sign-partnership-and-cooperation-agreement/> accessed 15 August 2023.
17. Raj A, 'A hole or a mole in Malaysian government agencies as another database leaked?' (*TechWire Asia,* 18 September 2022) <https://techwireasia.com/2022/09/a-hole-or-a-mole-in-malaysian-government-agencies-as-another-database-leaked/> accessed 15 August 2023.
18. Voss A, 'Position Paper on Fixing the GDPR: Towards Version 2.0' (*Axel Voss*, 25 May 2021) 30 <https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf> accessed 15 August 2023.