PROPHETIC LAW REVIEW
Volume 5, Issue 2, December 2023

PROTECTING OUR MOSTS VALUABLE PERSONAL DATA: A COMPARISON OF TRANSBORDER DATA FLOW LAWS IN THE EUROPEAN UNION, UNITED KINGDOM, AND INDONESIA

Budi Agus Riswandi[1], Alif Muhammad Gultom[2]

Citation Guide:
Budi Agus Riswandi, Alif Muhammad Gultom '**PROTECTING OUR MOSTS VALUABLE PERSONAL DATA: A COMPARISON OF TRANSBORDER DATA FLOW LAWS IN THE EUROPEAN UNION, UNITED KINGDOM, AND INDONESIA**' [2023] 5 (2) Prophetic Law Review 179.

Received:
4 December 2023
Accepted:
1 February 2024
Published:
25 February 2024

DOI:
10.20885/PLR.vol5.iss2.art3

Abstract

Information technology and its relationship with data protection is a crucial area that needs to be addressed, especially for data flows among different countries. In the majority of jurisdictions, international data transfers are restricted unless specific requirements stipulated by data protection laws are met. However, in the European Union (EU) and the United Kingdom (UK) there are three exceptions, adequacy, appropriate safeguards, and derogations. This paper conducts a comparative legal analysis of the regulations governing the cross-border transfer of personal data in the EU, UK, and Indonesia. The research method is normative, while the approaches employed are statutory and conceptual with an analytical and descriptive research design. The study focuses on the legal framework and the various mechanisms to protect personal data during transborder flows. The research identified both commonalities and disparities in data protection regulations in Indonesia, the EU, and the UK. Notably, differences appeared in the application of appropriate safeguards and the use of criminal sanctions in Indonesia. Finally, the study concludes by providing recommendations for future developments in the legal frameworks for cross-border data transfer in the EU, UK, and Indonesia.

Keywords: *Adequacy Decision, Cross-border Data Transfer, Personal Data Protection Law.*

A. Introduction

Data protection is a critical issue that requires critical attention. Information technology has become a necessity for everyone. As a matter of fact, there are 5.07 billion internet users in the world, most of whom are social media consumers.[3] As of July 2022, there were 2.93 billion active users of

[1] Professor, Department of Private Law, Universitas Islam Indonesia. E-mail: budiagusr@uii.ac.id
[2] Student of University College Cork, Ireland. E-mail: 122109665@umail.ucc.ie
[3] Keith Kakadia, 'A Comprehensive List of Social Media Statistics for Journalists' (*Sociallyin*, 30 March 2023) <https://blog.sociallyin.com/social-media-statistics-for-journalists-by-sociallyin>.

Facebook,[4] 500 billion tweets made per day,[5] and 1.440 billion members of Instagram.[6] The direct consequence of all of these users is that individuals produce 2.5 quintillion bytes worth of data daily. It is inevitable that companies and governments view personal data as valuable assets. For example, companies like Facebook or Google can use the data of their users to offer certain products based on the collected and processed data. When the world population exceeds 8 billion, even more data will be generated, requiring more innovation, and offering more potential for errors and resulting in more broad implications.

According to the World Economic Forum, the rising volume of personal data has created a new wave of opportunities for economic and social value creation.[7] However, threats to data security have been exposed by Edward Snowden's revelations in 2013 and other cases of data leaks such as Cambridge Analytica and Facebook in 2018 and Uber in 2017.[8] Therefore, the transfer of personal data has become one of the most controversial issues of data protection,[9], and the legal framework created by the government to protect personal data has been issued in each country, although producing different approaches. The General Data Protection Regulation ("GDPR") is one of the world's most comprehensive data protection legislation. It has become a model for many other data protection laws worldwide.[10] It was introduced to address the issue of protecting the privacy of citizens' information in the European Union ("EU") and replaced the Data Protection Directive 95/46/EC in 1995.[11] This regulation imposes requirements on all data controllers or

[4] Daniel Shvartsman, 'Facebook: The Leading Social Platform of Our Times' (*investing.com*, August 2023) <https://www.investing.com/academy/statistics/facebook-meta-facts/>.

[5] David Sayce, 'The Number of Tweets per Day in 2022' (*dsayce.com*, 2022) <https://www.dsayce.com/social-media/tweets-day/>.

[6] Quixy Editorial Team, '80+ Eye-Opening Social Media Statistics for Every Channel' (*quixy.com*, August 2023) <https://quixy.com/blog/social-media-statistics-for-every-channel/>.

[7] Kean Birch, Dt Cochrane and Callum Ward, 'Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech' (2021) 8 Big Data & Society 1 <http://journals.sagepub.com/doi/10.1177/20539517211017308>.

[8] Andrew J Hawkins, 'Uber Admits Covering up Massive 2016 Data Breach in Settlement with US Prosecutors' (*theverge.com*, 25 July 2022) <https://www.theverge.com/2022/7/25/23277161/uber-2016-data-breach-settlement-cover-up>.

[9] Danijela Vrbljanac, 'Personal Data Transfer to Third Countries – Disrupting the Even Flow?' (2018) 4 Athens Journal of Law 337 <https://www.athensjournals.gr/law/2018-4-4-4-Vrbljanac.pdf> 301, 338.

[10] Damien Geradin, Dimitrios Katsifis and Theano Karanikioti, 'GDPR Myopia: How a Well-Intended Regulation Ended up Favoring Google in Ad Tech' [2020] SSRN Electronic Journal 40 <https://www.ssrn.com/abstract=3598130>; Mark Taylor, *Genetic Data and the Law: A Critical Perspective on Privacy Protection* (1st edn, Cambridge University Press 2012) <https://www.cambridge.org/core/product/identifier/9780511910128/type/book>.

[11] 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), OJ 2016 L 119/1 24.05.2016 [Hereinafter as GDPR]; Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (1st ed. 2016, Springer International Publishing : Imprint: Springer 2016).

processors who do business inside the EU or deal with the personal information of EU people. [12] In the United Kingdom, the Data Protection Act of 2018 is the UK's implementation of the GDPR, and they still retain the law of the GDPR in identical form even though they are no longer an EU member state.[13] The only areas in which the EU and the UK-GDPR vary significantly are those about the most important aspects of national security, intelligence services, and immigration.

The personal data protection framework development is evolving in all jurisdictions, including Indonesia. As a country that also recognizes the significant value of personal data and the responsibility protect it, the Personal Data Protection Law was enacted in October 2022 to introduce new significant obligations for data controllers and processors that use personal data located in Indonesia.[14] Indonesia became the fifth country in Southeast Asia to legislate data protection. Malaysia, Singapore, the Philippines, and Thailand constituted the remaining nations.[15] There are hundreds of personal data protection laws around the globe, which differ in each jurisdiction.

Most of the aforementioned legal frameworks regulate the data subject and how it is being controlled and/or processed. In sum, the goal of the Data Protection Act is to guarantee recognition and respect of the value of personal data, as well as to safeguard the personal protection rights of individuals and to raise public awareness.[16] Since the majority of laws only apply in the same jurisdictions as the related laws, for example, GDPR only applies to companies or entities that process data from the EU or European Economic Area ("EEA").[17] Similarly, the United Kingdom's and Indonesia's laws only apply in their respective state authorities. The main concern is determining which rules and regulations would apply if an organization decided to move its data to a location outside of the state.

[12] GDPR (n 11) Art. 3.

[13] United Kingdom Data Protection Act (2018) [Hereinafter as UK DPA].

[14] Glenn Wijaya, 'Residual Issues in Indonesia's Forthcoming Personal Data Protection Law' (*iapp.org*, 18 August 2022) <https://iapp.org/news/a/residual-issues-in-indonesias-forthcoming-personal-data-protection-law/>.

[15] Ady Thea DA, 'Advokat Ini Ingatkan 3 Ketentuan Transfer Data Pribadi Ke Luar Negeri' (*hukumonline*, 4 October 2022) <https://www.hukumonline.com/berita/a/advokat-ini-ingatkan-3-ketentuan-transfer-data-pribadi-ke-luar-negeri-lt633baec525388/>.

[16] Michael Pisa, Pam Dixon and Ugonma Nwankwo, 'Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity' (*center for global development*, 11 August 202AD) <https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and>.

[17] GDPR (n 12).

Nowadays, data transfers between companies have been common, including those with overseas branches or parent companies.[18] For example, with the use of pervasive media,[19] personal data of an individual or company can be transferred internationally to foreign platforms. Data exchanges on the borderless platform have increased in the cyberspace world, and it does not stop with the initial data when the data is sent, and continue to grow and develop along with the activities and movements in question.[20] Briseida (2021) in her paper, explains how to transfer data between the EU and U.S., especially within the GDPR framework that restricts the transfer outside of the EU.[21] Her paper argues that The International Principles on the Application of Human Rights to Communications Surveillance255 (2014) is a good start for this issue.[22] In a study conducted by Edoardo (2021), he examined how data movement across borders was affected after the UK departed from the EU.[23] The researchers concluded that Brexit made data protection law more complicated. This is because it led to the creation of two separate sets of laws that could potentially impact the same individuals or organizations.

Currently, Indonesia is still in the early stages of establishing data protection laws, and there are significant gaps, particularly when it comes to regulating the transfer of data outside the country's jurisdiction. Notably, there have been no legal cases or judicial interpretations specifically addressing the articles related to cross-border data flows. The existing laws do not provide clear standards or guidance on how foreign laws should be recognized under Indonesian law. Hence, this paper addresses the transborder or international personal data transfer issue under the prevailing regulations in the EU, UK, and try to compare them with Indonesia. The comparison between the UK and EU was chosen because these two regions are considered pioneers in the field of data protection, with the GDPR being a well-known and comprehensive law in this area. Furthermore,

[18] Svetlana Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two "Necessities"' (2020) 21 The Journal of World Investment & Trade 881, 890 <https://brill.com/view/journals/jwit/21/6/article-p881_4.xml>.

[19] Over-the-Top (OTT) are media services that are delivered directly to viewers over the Internet (e.g. Netflix, Disney+, Amazon Prime Video).

[20] Jos Dumortier and Caroline Goemans, 'Data Privacy and Standardization' (CEN/ISSS Open Seminar on Data Protection, Brussels, 23 March 2000) <https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/90cen-paper2f90.pdf>.

[21] Briseida Sofía Jiménez-Gómez, 'Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute' (2021) 19 Santa Clara Journal of International Law 45 <https://digitalcommons.law.scu.edu/scujil/vol19/iss2/1>.

[22] Briseida Sofía Jiménez-Gómez (n 21) 45.

[23] Edoardo Celeste, 'Cross-Border Data Protection After Brexit' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3784811>.

previous legal cases in both jurisdictions provide valuable insight into how judges have interpreted the issue of transborder data transfers.

This begins by addressing the importance of international personal data transfers by entities and their consequences. It compares and contrasts the legal frameworks in the three mentioned jurisdictions. Following that, it explores the penalties for non-compliance with these laws, concluding with an overview of the current challenges in international data transfers.

B. Methodology

In order to narrow down the focus of this research, the problem formulations for this research are as follows: How important is it to regulate international data transfers, and what drives entities to engage in such cross-border transactions? How do the regulations governing personal data transfer in the EU, UK, and Indonesia differ, and what commonalities exist among these jurisdictions?

The study employs a normative legal methodology through a combination of statutory and conceptual approaches. Secondary sources were used and obtained from primary, secondary, and tertiary legal materials. The sources used in the research were obtained from a variety of legal materials including international agreements, books, articles, and legal journals, as well as dictionaries to clarify certain terms. The research utilized a descriptive qualitative method to analyze factors related to the research object, which aimed to provide more in-depth data.

C. Discussion and Results

1. The Urgency of Transferring Personal Data in Electronic Transactions

International data transfer essentially concerns the transfer of personal data to another country or jurisdiction. Transferring data across international borders is a crucial component of day-to-day business operations for any company that does business worldwide. The scope of the company's data transfer activities is very broad and varied by the subject matter. Cloud technology, web-based services, and other components of the Internet of Things are examples of data transfers that can occur in the context of transborder or international personal data transfer.[24] For example, entities may retain

[24] Veronika Stoilova, 'Regulation of International Data Transfers under EU Data Protection Law' (2021) 13 CES Working Papers 16 <https://ceswp.uaic.ro/articles/CESWP2021_XIII1_STO.pdf>.

customer data in a cloud service hosted in another nation or store employee data in a subsidiary created in a different country, which falls under international data transfer.[25] International data flows are necessary for international trade and international cooperation between countries. As a matter of fact, in 2019, the United Kingdom digitally exported more than £200 billion worth of services, and this trend is expected to continue growing.[26]

As mentioned, 2.5 quintillion bits of data are generated daily, and cross-border connection supports innovation and employment growth for all businesses and individuals.[27] The statistics of data growth has seen even more rapid growth since 2021, mainly due to the covid-19 global pandemic. During the pandemic lockdown, everyone was required to shelter in place. However, some activities, such as education and employment, could not be suspended. Under these conditions, everything had to be completed remotely using online platforms and digital methods. This has had a significant influence on the growth of data, which has since been on the increase.[28] Further, Francesca and Javier's paper 'Trade and Cross-border data flows' research submits that data transfers contributed 2.8 trillion USD to global GDP,[29] and it is growing 45 times every ten years.[30]

The health research sector is significantly dependent on data transfer. Various data from different jurisdictions helps health researchers obtain sufficient large study numbers to ensure that the research is relevant for patients across the globe. Ultimately, global health information data sharing is critical to maximizing the individual and social

[25] Yunchuan Sun and others, 'Data Security and Privacy in Cloud Computing' (2014) 10 International Journal of Distributed Sensor Networks 1, 2 <http://journals.sagepub.com/doi/10.1155/2014/190903>.

[26] Department for International Trade and The Rt Hon Anne-Marie Trevelyan MP, 'Digital Trade Key to Unlocking Opportunities of the Future' (*gov.uk*, 25 November 2021) <https://www.gov.uk/government/news/digital-trade-key-to-unlocking-opportunities-of-the-future>.

[27] Global Data Alliance, 'Cross-Border Data Transfers & Privacy' (*globaldataalliance.org*, May 2020) <https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf>.

[28] Gemma Newlands and others, 'Innovation under Pressure: Implications for Data Privacy during the Covid-19 Pandemic' (2020) 7 Big Data & Society 1, 2 <http://journals.sagepub.com/doi/10.1177/2053951720976680>.

[29] Francesca Casalini and Javier López González, 'Trade and Cross-Border Data Flows' (2019) 279 OECD Trade Policy Papers 40 <https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1708021350&id=id&accname=guest&checksum=2688193BC4BEC9C4BF22813D40F2F04E>; Colin J Bennett and Charles D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2nd and updated ed. edn, MIT Press 2006).

[30] Francesca Casalini and Javier López González (n 29)

advantages of study participants' contributions.[31] Especially during the Covid-19 pandemic, external laboratories and data exchanges can help the vaccine creation process. Dr. Robin Fears, one of the lead medical researchers[32] added that "International sharing of data for research is often particularly important, for example, to compare the determinants and outcomes of disease in different settings, to assess whether findings in other countries are also applicable to patients in Europe, and to capitalize on the emergence of new big data sets."[33]

Based on the above argument, worldwide data transmission across borders is critical in the rapidly evolving technology of today's society and how personal data is valued. Therefore, this becomes an important part of being governed by a set of rules considering the value and the risk of misuse by irresponsible entities. There must be assurance that personal data transmitted to foreign territory receives the same level of protection as in the country of origin. This avoids scenarios in which the receiving country has inadequate personal data protection rules, possibly resulting in the unrestricted use of personal data sent to that country. Without proper restrictions, it could be possible for individuals to use the gap to store personal data in countries with no personal data privacy standards, therefore avoiding the limits of the rules of protection. This is also recognized by Millard (1985):

> *Just as money tends to gravitate towards tax havens, so sensitive personal data will be transferred to countries with the most lax [sic.], or no data protection standards. There is thus a possibility that some jurisdictions will become 'data havens' or 'data sanctuaries' for the processing or 'data vaults' for the storage of sensitive information.*[34]

Subsequently, most governments' legislation has also aimed to address the cross-border data flow. However, diverse responses to this problem exist, and no one universal

[31] ALLEA (European Federation of Academies of Sciences and Humanities), FEAM (Federation of European Academies of Medicine), and EASAC (European Academies' Science Advisory Council), *International Sharing of Personal Health Data for Research* (ALLEA 2021) <https://doi.org/10.26356/IHDT>..

[32] Dr. Robin Fears one of the lead authors of the Allea (All European Academies) Report concerning international sharing of personal health data for research.

[33] ALLEA, 'Sharing Matters: Why International Data Transfer Is Crucial For Health Research' (*ALLEA (European Federation of Academies of Sciences and Humanities)*, 26 April 2021) <https://allea.org/sharing-matters-why-international-data-transfer-is-crucial-for-health-research/>.

[34] Christopher J Millard, *Legal Protection of Computer Programs and Data* (Carswell Co ; Sweet & Maxwell 1985) 211; Ian J Lloyd, *Information Technology Law* (9th edn, Oxford University Press 2020) 185.

model for regulating it exists.[35] Due to different legal and regulatory frameworks, international data transfer has always been complicated. For example, in the United States, they have no restrictions on the transfer of personal data to foreign jurisdictions, although trying to protect several data breach cases.[36] On the other hand, most other countries allow international data transfer with strict restrictions. In China, personal information can be transferred internationally only if consent has been obtained, an assessment conducted, and other specified conditions under the PIPL.[37] In Russia, following the latest amendment 266-FZ, there is an additional requirement to inform the regulatory body of their purpose for conducting a cross-border data transfer.[38]

The rules of GDPR on data transfer to other non-EU countries are stated under Chapter 5 concerning transfers of personal data to third countries or international organizations.[39] Therefore, to move data outside of the EU, it is necessary to justify the transfer under the options provided, e.g., adequacy decision, appropriate safeguards and finally, derogations, which will be explained thoroughly in the next section. This is similar to the standard applied by the United Kingdom, which follows Chapter 5 of the GDPR. Indonesia, on the other hand, proposed three alternative criteria that a processor or controller must fulfil.[40]

In general, many alternative approaches are available to manage data transfers across international borders. International data transfer cannot be avoided as the current volumes of cross-border transfer occurring every moment and the positive outcome can be achieved. In essence, each nation has its own rules and criteria to ensure that data sent beyond its jurisdiction remains secure.

2. Cross-Border Transfers of Personal Data Under The GDPR

[35] UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (*unctad.org*, April 2016) <https://unctad.org/publication/data-protection-regulations-and-international-data-flows-implications-trade-and>.

[36] Michael T Hubbard, 'Personal Data of U.S. Citizens Transferred Abroad Needs Protection' (*natlawreview*, 30 July 2019) <https://www.natlawreview.com/article/personal-data-us-citizens-transferred-abroad-needs-protection>.

[37] Jet Zhisong Deng and Ken Jianmin Dai, 'China's Restrictions on Cross-Border Transfer of Personal Information: An Update on Regulatory Policy and Practical Implications' (*ibanet*, 17 February 2023) <https://www.ibanet.org/chinas-restrictions-on-cross-border-transfer-of-personal-information>.

[38] Anas Baig, 'What To Know About The Russian Federal Law No. 152-FZ' (*securiti.ai*, 5 August 2023) <https://securiti.ai/russian-federal-law-no-152-fz/>.

[39] GDPR (n 11) Art. 44.

[40] Indonesia Law No. 27 of 2022 on Personal Data Protection Law, Art. 56

Europe, via its supranational organizations, serves as a launching pad for the most comprehensive worldwide projects pertaining to this data protection sector. [41] Historically, GDPR was preceded by two important pieces of legislation on data protection. The first was the OECD (Organization for Economic Co-operation and Development), an international organization that has published several influential data protection agendas, such as the 'Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data in 1980.[42] The second was the EU Data Protection Directive 1995, which governed the seven principles in the OECD Recommendations. The level of enforceability and the precise enforcement methods that EU members may utilize to meet data protection obligations are the primary areas in which the GDPR differs significantly from its two data protection predecessors.[43]

The GDPR provides ground rules for the protection of natural people's privacy in relation to how the processed and free movement of personal data should be.[44] Although it is a European Law, it aims to preserve the right to privacy for all EU citizens, and therefore all websites and/or services in the world that process the European's personal data must comply with the GDPR's provisions. There are just a few limitations on data transfer inside the EEA, including the obligation to notify the transfer of tax information and data transfer regarding national security. Under its significant provisions, GDPR governs the flow of data when it is being transferred to a country that is not a member of the EU, especially in this globalized world where the data stored on servers in different countries.

Chapter V of the GDPR regulates how the data transfer from the EU to non EU countries or international organization can be legally permitted. The three alternative

[41] Lee A Bygrave, *Data Privacy Law: An International Perspective* (1st edn, Oxford University Press 2014) <https://academic.oup.com/idpl/article-abstract/5/1/88/622973>; GW Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (1st edn, Oxford University Press 2014).

[42] Nate Lord, 'What Is the Data Protection Directive? The Predecessor to the GDPR' (*digitalguardian.com*, 28 December 2022) <https://www.digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr>; Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University PressNew York 2020) <https://academic.oup.com/book/41324>.

[43] Brian Daigle and Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' [2020] Journal of International Commerce and Economics 38; Eduardo Ustaran (ed), *European Data Protection: Law and Practice* (an IAPP Publication, International Association of Privacy Professionals 2018).

[44] Chris Jay Hoofnagle, Bart Van Der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65, 66 <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501>; William Mcgeveran, *Privacy and Data Protection Law* (2nd edn, Foundation Press 2023).

legal grounds are transfers based on adequacy decisions, adequate or appropriate safeguards, and derogations.

a. Adequacy Decisions

An adequacy decision is a formal and legally binding decision made by the EU Commission[45] where it has determine that the country has the same or equivalent level of data protection as the EU.[46] The decision involves an opinion from the European Data Protection Board, approval from representatives of EU countries, and a proposal along with the adoption by the European Commission.[47] The decision should be based on two primary considerations, namely, the substance of the relevant regulations of the third country and the mechanism for guaranteeing the effectiveness of such rules. Furthermore, the GDPR also stated that the decision may be cancelled or maintained by the European Parliament and the Council at any time.

Currently, several countries have been recognized based on adequacy decisions, including Argentina, Andorra, Faroe Islands, Japan, New Zealand, and Switzerland.[48] Therefore, any EU personal data may travel from the EU to these nations without additional protections. The US was also a member of this group but was removed from the list by the latest CJEU judgement.[49]

b. Appropriate Safeguards

Where countries do not qualify for an adequacy determination, they must seek an alternative mechanism to provide appropriate safeguards for EU citizens' data. These include binding corporate rules, standard contractual clauses, and approved codes of conduct. First, Binding Corporate Rules ("BCR") are a set of rules between a group of companies under the same parent on how to protect the personal data of employees, clients, and other individuals of the EU. This rule is designed to enable a company to transfer personal data from the EU to affiliates situated outside of the territory in conformity with the GDPR. This is created by the company and is then

[45] The European Commission is the executive branch of the European Union (EU) and is responsible for proposing legislation, implementing decisions, and upholding the EU treaties

[46] GDPR (n 11) Art. 45

[47] Alexandra Maria Rodrigues Araújo, 'The Right to Data Protection and the Commissions' Adequacy Decision' (2015) 1 UNIO – EU Law Journal 77, 81 <https://revistas.uminho.pt/index.php/unio/article/view/286>.

[48] List of third countries which ensure an adequate level of protection can be seen through: General Data Protection Regulation (GDPR), 'GDPR Third Countries' <https://gdpr-info.eu/issues/third-countries/>.

[49] CJEU - C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559

examined by the EU Member State regulatory agencies before being submitted to the European Data Protection Board ("EDPB") for final approval. Once the EU authority approves a BCR, it becomes legally binding, and the company can use the rules to transfer personal data outside of the EU without further authorization.

The second category is Standard Contractual Clauses ("SCC"), which apply when one party is a controller, and the other is a processor. The EU Commission has produced a model for contractual provisions that companies may employ on a voluntary basis in their contractual arrangements with third parties. Because of their simplicity of use, SCCs are one of the most often utilized techniques for transferring personal data to third countries outside the EU/EEA. Under the standard, it includes several types of relationships and the responsibility of each party. The EU Commission SCC is based on Directive 95/46/EC until the Schrems II judgment invalidated the Privacy Shield between the US and EU concerning data protection transfer. Schrems II is a landmark case between the Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems in 2020 that was decided by the Court of Justice of the European Union. Maximillian Schrems, the complainant, asserted that Facebook's transfer of personal data to its headquarters in the US might be accessible by US intelligence services, which was a violation of the GDPR and EU law. He called for the Irish Data Protection Commissioner to invalidate the SCC used by Facebook, which is known as the EU-US Privacy Shield. The outcome is that the Court of Justice agreed with Schrems and ruled that the EU-US Privacy Shield determination was invalid.

Following the case, the EU released its new standards, which requires parties first to evaluate the risk of transferring personal data to a third country and take necessary measures if access to that data is required. However, the court emphasized that the company that still relies on the previous SCC and must ensure on a case-by-case basis that the transfer of personal data is equivalent to the EU's protections. The third mechanism of appropriate safeguards is through the approved code of conduct, which falls under Articles 40 and 41 of GDPR.

Codes of conduct are usually used by different processing sectors and micro, small, and medium-sized enterprises. It helps them to apply EU data protection law requirements to specific issues. Codes are expected to provide added security for their sector as they will address the requirements for data processing. Under this measure,

it starts with a submission of a draft code to the supervisory authority to be approved. The body then assesses whether the code already complies with appropriate safeguards and, therefore, monitors compliance with the code. In practice, however, the authorized code of conduct is unlikely to be utilized, the European Data Protection Board (EDPB) has published specific instructions relating to the regulation addressing both Codes of Conduct and Monitoring Bodies under Articles 40 and 41 GDPR, that offer more clarity to the procedure. Based on the three safeguards above, the author believes that the practical and more suitable way for company to use is the standard contractual clauses as a basis for transfer between different entities while BCR is to be used for the multinational groups.

c. Derogations

Under the GDPR, the last option when a country cannot provide an adequate level of protection or appropriate safeguards, is a number of derogations provided in the regulations.[50] There are six conditions that are permitted under Article 49 of the GDPR; this paper examines each situation. First is explicit consent. There are three thresholds for the first condition to be met, which are the consent must be explicit, it shall be specific for the particular data transfer/set of transfers, and the person who gives the data must be informed particularly as to the possible risks of the transfer.[51] Second, when the transfer is necessary for the performance of a contract between the subject parties. the EPDB further suggests that for a data transfer to be considered 'necessary,' there must be a 'close and significant relationship' between the transfer and the contract's stated goals.[52] Third, the transfer must be important for public interest. In this instance, public interest is only applicable where the controller is subject to a significant public interest in the spirit of global co-operation. The existence of international agreements might become a recognized indicator.[53]Fourth, derogation is provided for to exercise legal claims. Legal claims cover various actions in the context of an administration or criminal investigation in the third country. Data transfer for pre-trial in civil litigation may also fall under this derogation. Fifth, the

[50] GDPR (n 11) Art. 49.

[51] European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018* (EDPB 2018) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf>.

[52] European Data Protection Board (n 51).

[53] European Data Protection Board (n 51).

transfer is to protect the vital interest of the data subject. An example of this situation is when the data subject is unconscious, and the exporter is the only person who can provide the data; a derogation may be granted (usually for a medical emergency).[54] However, once the subject is able to make reasonable decisions, derogation might no longer be justified. Sixth, the last legitimate derogation is when a transfer is made from a public register.[55] The relevant registry must, in accordance with the laws of the Union or the Member States, be designed to make information available to the general public.

GDPR is a last-resort basis for transferring data if none of the above situations are applicable. However, it should be under the condition that the transfer is not repetitive, and concerns only a limited number of data subjects, provided by suitable safeguards and for the purpose of compelling legitimate interests.[56] The regulatory authority must always be informed whenever a transfer of this kind occurs. In sum, derogations are more difficult to use and need legitimate justification.

Based on the above rules, the GDPR allows the international transfer of personal data beyond the EU as long as it complies with the guidance provided under Chapter V, although the data processor also needs to apply the other relevant provisions under the GDPR. One of the biggest challenges faced by global organizations operating in the EU is finding the right mechanism to allow data movements of EU citizens' data, and it can be time-consuming. However, despite technological developments and greater globalization, it is unlikely that the EU will relax its approach in the foreseeable future, considering the current rigid regulatory scheme.

3. Processing and Supervision Method of International Data Transfer in The United Kingdom

As the United Kingdom adopted the GDPR into its national law and has a data protection law that is quite the same as EU provisions, this section will focus on the differences between the UK GDPR and the EU on the international data transfer method. Historically, the UK introduced its own Data Protection Act in 2018, and the EU GDPR came into effect. Due to the present Brexit agreement, the only applicable legislation is the GDPR of the United Kingdom, which is a combination of the GDPR of the European

[54] European Data Protection Board (n 51).
[55] GDPR (n 11) Art. 49 (1) (g)
[56] GDPR (n 11) Art. 49 (1)

Union and the Data Protection Act. The UK GDPR has similar provisions to the EU GDPR, establishing key definitions and fundamental data protection principles pertaining to data processing, as well as particular accountability and limits for data transfers outside of UK jurisdictions. International data transfer is set out under Articles 45 to 49 of Chapter V, which consist of adequacy decisions, safeguards, and several derogations.

a. Adequacy Decisions

Similar to the provisions set out in the EU GDPR, the UK allows restricted transfer based on adequacy decisions for the countries that are published by the UK Home Secretary.[57] The government will conduct the assessment concerning the level of data protection in the related countries, and once it passes this step, a recommendation will made by the Home Secretary to the Parliament.[58] Currently, the adequacy decisions given to the countries, including in the European Economic Area, Gibraltar, territory and sectors covered by European Commissions adequacy decisions, Republic of Korea and partial findings upon Japan and Canada. Additionally, countries such as Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay have also received adequacy decisions.[59]

As the United Kingdom is no longer a member of the EU, the government has stated in an official announcement that it would negotiate data adequacy decisions with international partners and reduce barriers to international data flows by providing alternative data transfer mechanisms.[60] Presently, the UK has identified ten countries as its 'priority destinations' for such deals.[61] This scheme demonstrates that the UK would want to make space for differentiations with the EU protection legislation while

[57] United Kingdom Data Protection Act (n 13) s 17.

[58] Ryan Chiavetta, 'UK Announces Independent Adequacy Decisions; Edwards Named ICO Top Candidate' (*iapp.org*, 26 August 2021) <https://iapp.org/news/a/uk-announces-independent-adequacy-decisions-edwards-named-ico-top-candidate/> accessed 2 January 2023.

[59] Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (*ico.org.uk*, 14 October 2022); Information Commissioner's Office, 'International Data Transfers' (*ico.org.uk*) <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/>; Daniel Rücker and Tobias Kugler, *New European General Data Protection Regulation, a Practitioner's Guide: Ensuring Compliant Corporate Practice* (CH Beck Hart publishing Nomos 2018).

[60] 'UK Approach to International Data Transfers' (26 August 2021) <https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers>.

[61] The country includes Australia, Brazil, Columbia, The Dubai International Financial Centre, India, Indonesia, Kenya, The Republic of Korea, Singapore and the U.S.

maintaining the GDPR as the basis. In future, the UK approach is to design globally interoperable transfer mechanisms.[62]

b. UK Safeguards

One of the safeguards that differs between the standards applied in the EU and the UK is concerning the Standard Contractual Clauses. SCC is a set of clauses to be put in the counteract defined as a standard by the authority body so that the company may use it as a standardization. The UK, through its Information Commissioner Office, has issued a new SCC, which the International Data Transfer Agreement ("IDTA") and a new International Data Transfer Addendum to the European Commission SCCs (the "Addendum"). The EU standard and the IDTA are highly similar, differing only in the absence of Article 28 in the IDTA, which outlines the responsibilities of data processors. This creates a complicated patchwork of data transfer agreements. In addition, EU GDPR differs from four schemes of data transfer parties, which are controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller contracts. The IDTA consists of four different parts which are: (i) Tables related to parties and signatures, transfer details, transferred data, and security requirements; Part (ii) Extra Protection Clauses, technical, organizational, and contractual; Part (iii) Commercial Clauses; and Part (iv) Mandatory Clauses.

On the other hand, the Addendum is an 'add-on' of the new EU SCCs, and it produces short, clear, and flexible clauses. UK Addendum allows organizations to use the EU SCCs themselves to cover EU and UK transfers.

c. Derogations

The UK GDPR allows the data exporter to transfer personal data outside of the UK under the eight exceptions stated in Article 49. The derogations allow transfer in particular situations, such as based on consent, performance of a contract, exercise of legal claims, public interest, and to protect the vital interests of the data subject where they cannot give consent, which is quite similar to the exceptions under the EU GDPR. The UK Information Commissioner Office ("ICO") guidance on these derogations should always be consulted and informed to ensure that they can be relied upon for the situation organizations are address.

[62] 'UK Approach to International Data Transfers' (n 60).

One of the approved situations by ICO was made in 2019, which confirms that UK firms may rely on public interest derogations to transfer data to the U.S. Securities and Exchange Commission ("SEC"). Previously, the SEC requested UK-domiciled firms or branches registered by the SEC for its books, records, documents, and other information to make them available for inspection upon SEC staff's request. The information, which includes emails sent and received by employees, customer complaints, and financial transaction records, will likely include personal data. After conducting its analysis, ICO confirms that there are overlapping *'lines of public interest',* which benefit UK forms complying with SEC rules.[63] Nonetheless, the UK also mentioned that UK Firms should apply Article 46 if possible, and the derogations should only be used on a case-by-case basis.

4. Indonesian Personal Data Protection Law

After many years, Indonesia enacted a Personal Data Protection Law ("PDPL") on 17 October 2022.[64] The PDPL applies to personal data processed by electronic and non-electronic methods, in contrast to the former regulatory framework[65], which only concentrates on personal data processed via an electronic system. Besides the above regulations, Indonesia's data protection is also entitled under specific laws in a particular area, such as Personal data in the health sector is also governed under Ministry of Health Regulation No. 24 of 2022 on Medical Record, in banking area, it is regulated under Bank Indonesia Regulation No. 22/20/PBI/2020 regarding Protection of Bank Indonesia Consume, while for government administration, its governed under personal data collected under Law No. 23 of 2006, as amended by Law No. 24 of 2013 on Demographic Administration. In addition to the above, personal data protection was distributed across more than 30 different laws and regulations.[66] However, the regulations governing cross-border transfer are under the new PDPL, which this section will focus on.

[63] Hunton Andrews Kurth, 'ICO Confirms UK Firms May Rely on Public Interest Derogation for SEC Transfers' (*natreview.com*, 29 January 2021).

[64] Personal Data Protection Law (n 40); Jacqueline Klosek, 'Indonesia: A Long-Awaited Privacy Measure Finally Becomes Law In Indonesia' (*mondaq*, 16 November 2022).

[65] Indonesia Law No. 11 of 2008 on Information and Electronic Transactions.

[66] Hunter Dorwart and others, 'INDONESIA'S PERSONAL DATA PROTECTION BILL: OVERVIEW, KEY TAKEAWAYS, AND CONTEXT Indonesia's Personal Data Protection Bill: Overview, Key Takeaways, and Context' (19 October 2022) <https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/>; Rizky PP Karo Karo and Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat* (Nusa Media 2020).

According to the PDPL, it applies to any person, including people and businesses, as well as any governmental entity or international organization that carries out legal action contemplated under the PDPL and is located:[67]

(i) within the jurisdiction of Indonesia; and/or

(ii) outside the Indonesian jurisdiction, but its action has a legal impact:

a. in the jurisdiction of Indonesia; and/or

b. on Indonesian personal data subjects outside the jurisdiction of Indonesia.

In sum, the PDPL was drafted closely following the principle set down by the GDPR. The degree to which the two are comparable may be seen by comparing aspects such as data subject rights, legitimate basis for data processing, clearly stated fines, and data breach regulations. However, there are also significant variations between the two, including the authority of regulatory organizations, the scope of the rules, and the specific data covered by the laws.

Transfers across international borders are governed by Article 56 of the PDPL, which permits a data controller to transfer to another controller and/or processor outside of Indonesian jurisdictions if one of three conditions is satisfied. First, before moving personal data overseas, the personal data controller must guarantee that the country where the personal data controller and/or personal data processor will receive the data has a degree of personal data protection equivalent to or stronger than Indonesia's PDPL.[68] The law does not specify the standardization or explanation concerning the equal value of law with the Indonesian Law.

Second, if the receiving country that gets the information does not have standards that are equivalent to or higher than the PDP Law, the personal data controller must guarantee that there is appropriate and legally enforceable protection of personal data.[69] It is also possible to interpret it via contracts or other legally enforceable documents, making it such that data receivers are subject to Indonesian

[67] Siti Yuniarti, 'PROTECTION OF INDONESIA'S PERSONAL DATA AFTER RATIFICATION OF PERSONAL DATA PROTECTION ACT' (2022) 4 Progressive Law Review 54 <http://progresiflawreview.ubl.ac.id/index.php/plr/article/view/85>. Jihyun Park and Dodik Setiawan Nur Heriyanto, 'In favor of an Immigration Data Protection Law in Indonesia and Its Utilization for Contract Tracing'. [2022] 4 (1) Prophetic Law Review; Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-57959-7>.

[68] Personal Data Protection Law (n 40) Art. 56 (2)

[69] Personal Data Protection Law (n 68)

legislation.[70] Under the second clause, however, the law does not specify how contracts or other legally enforceable agreements should be structured, although further requirements will be contained in separate regulations.[71]

Third, in the event that these first two requirements are not satisfied, the controller of the personal data must get the consent of the subject of the personal data.[72] It seems that PDPL has a broader concept of exception compared to the GDPR without any further limitations. PDPL allows transfer with consent regardless of whether the receiver country has an equivalent or higher level of data protection to the PDP Law. Whilst under the GDPR, a controller can utilize a data subject's consent to transfer personal data to a jurisdiction without adequate measures and shall impose additional transparency obligations[73]

The three requirements are met in an alternative rather than cumulative way. Therefore, only one of the requirements may be met at a time. The PDPL in its last verse on Article 56 stated that further provisions regarding the transfer of personal data will be included in a separate regulation.

5. Penalties and Liabilities for Cross Border Violations in The European Union, United Kingdom, and Indonesia

The data protection law act in each jurisdiction imposes a tiered system for administrative sanctions, including fines, or even some of the law also provides criminal liabilities. These sections will focus on the sanctions upheld for non-compliance with the regulation by each jurisdiction.

a. European Union

According to the EU GDPR, there are significant administrative penalties for non-compliance with the legislation. It allows Data Protection Authority ("DPA") to impose fines on the controller (entity responsible for data processing),[74] and the processor entity that processed the data on behalf of the controller.[75] Article 83 of GDPR divides the two tiers of administrative fines, which are (i) Up to €10 million,

[70] Ady Thea DA, 'Advokat Ini Ingatkan 3 Ketentuan Transfer Data Pribadi Ke Luar Negeri' (*hukumonline*, 4 October 2022) <https://www.hukumonline.com/berita/a/advokat-ini-ingatkan-3-ketentuan-transfer-data-pribadi-ke-luar-negeri-lt633baec525388/>.

[71] Personal Data Protection Law (n 40) Art. 56 (5)

[72] Personal Data Protection Law (n 40) Art. 56 (4)

[73] GDPR (n 11) Art. 49

[74] GDPR (n 11) Art. 4 (7)

[75] GDPR (n 11) Art. 4 (8)

or 2% of annual global turnover or (ii) Up to €20 million, or 4% of annual global turnover. These fines are based on the types of non-compliance with data processing, storage, and data breach notification requirements set out in the regulations.

In addition, GDPR also allows member states to choose to provide for criminal sanctions under their national laws, but it is not a requirement under the GDPR. The GDPR focuses on imposing administrative fines and sanctions, such as warnings, reprimands, or prohibitions on carrying out certain activities, on both natural and legal persons in case of non-compliance. It is important to note that GDPR enforcement is the responsibility of the supervisory authorities of each EU member state, so the level of enforcement may vary.

Since the GDPR came into effect in May 2018, several high-profile fines and penalties have been imposed by supervisory authorities across the EU.[76] The fines and penalties have been imposed on a variety of organizations, including large multinational companies, small and medium-sized businesses, and public sector bodies. Some of the most significant fines under the GDPR include the case of Google, which was fined €50 million by the French data protection authority CNIL, the case of a German social media company, which was fined €20,000 by a German court for failing to appoint a data protection officer and the case of Facebook that received an administrative fine of billion euros because failure to disclose the data breach to the regulator in a timely manner.[77] The fines and sanctions are determined on a case-by-case basis and take into account the specific circumstances of each case.

b. United Kingdom

The UK's GDPR provides several different types of sanctions for non-compliance, including fines and enforcement notices. The UK's ICO has the power to impose fines of up to £17.5 million or 4% of a company's global annual revenue, whichever is greater, for certain types of violations, such as failure to comply with a data protection supervisory authority's order or failure to report a data breach. For less severe violations, such as failure to appoint a Data Protection Officer or failure to

[76] Josephine Wolff and Nicole Atallah, 'Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020' (2021) 11 Journal of Information Policy 63, 64 <https://scholarlypublishingcollective.org/informationpolicy/article/doi/10.5325/jinfopoli.11.2021.0063/291999/Early-GDPR-Penalties-Analysis-of-Implementation>; European Union Agency for Fundamental Rights. and others, *Handbook on European Data Protection Law: 2018 Edition.* (Publications Office 2018) <https://data.europa.eu/doi/10.2811/343461>.

[77] Wolff and Atallah (n 76) 65.

conduct a Data Protection Impact Assessment, fines may be up to £8.7 million or 2% of global annual revenue.[78] The ICO can also issue enforcement notices, which require organizations to take specific steps to comply with the UK GDPR, such as providing training for employees or implementing new security measures. Organizations that fail to comply with an enforcement notice can be fined.

The fines and sanctions for non-compliance ICO are meant to be proportional to the severity of the violation and the size and revenue of the company. It is also determined on a case-by-case basis, the same as under the EU GDPR. The ICO has imposed several fines under the GDPR since it came into effect in 2018. Some of these fines have been significant, such as the £183 million fine imposed on British Airways for a data breach in 2018 and the £500,000 fine imposed on Facebook for its role in the Cambridge Analytica scandal.[79] The number of fines continues to investigate and enforce compliance with the regulation.

c. Indonesia

The PDPL of Indonesia provides several different types of sanctions for non-compliance, including fines and imprisonment. The PDPL prescribes the administrative sanctions and criminal liability that increase depending on the severity of the penalty. As for administrative sanctions, the Indonesian Data Protection Authority may impose (i) a written warning; (ii) temporary suspension of processing activities; (iii) forced deletion of personal data; and/or (iv) administrative fines of a maximum of two percent of annual income or annual revenue for violation variables.[80]

The second category is for persons or businesses that do unlawful acts. Articles 67 to 73 of the PDPL prohibit, among other things, the collection, disclosure, and falsification of personal information for financial gain, resulting in damages for others. It stipulates that anyone who intentionally or unlawfully obtains, collects and uses personal data belonging to others will be liable to a fine of 5 billion rupiahs and/or a maximum prison sentence of 5 years.[81] Those who disclose information in a similar way face up to four years in prison and/or a fine of up to 4 billion Rupiah.[82] Individuals

[78] Wolff and Atallah (n 76).

[79] Mona Naomi Lintvedt, 'Putting a Price on Data Protection Infringement' (2022) 12 International Data Privacy Law 1 <https://academic.oup.com/idpl/article/12/1/1/6453860>.

[80] PDPL (n 40) Art. 57

[81] PDPL (n 40) Art. 67 (1)

[82] PDPL (n 40) Art. 67(2)

and organizations that willfully create false data may face a six-year jail sentence, a maximum fine of 6 billion rupiah, and/or the confiscation of assets earned via unlawful conduct.[83]

If a corporation commits the aforementioned offenses, only penalties may be levied.[84] Criminal penalties for corporations may be up to 10 times the maximum penalties for individuals.[85] Besides, corporations may also be subject to other punishments, including seizure of earnings or assets earned via illegal activity; Cancellation of permits, commercial activities, or physical locations; and/or Dissolution of the company or permanent prohibition of certain activity.

In addition to the above, the PDPL specifies the methods and deadlines for dealing with a criminal penalty, such as sanctions for failing to pay or settling disputes with auctioned property.[86] As the PDPL has only recently been enacted, and the government is still in the process of forming the data protection authority, there is no current case concerning data protection breach of the new law. Furthermore, the PDPL still has a two-year implementation grace period for Controllers, Processors, and other relevant parties that handle personal data.

6. Comparative Findings

Based on the above elaboration above, the author has identified both differences and similarities in the approaches to cross-border transactions in Indonesia, the UK, and the European Union. One notable similarity is that all three countries impose significant restrictions when it comes to regulating cross-border transfers between distinct jurisdictions, even though they ultimately allow these transactions to take place.

The EU and the UK share a largely similar approach due to the UK's previous membership in the EU. During the United Kingdom's membership in the European Union, it was obligated to adhere to and observe EU regulations. Consequently, when the GDPR was introduced in 2018, the UK incorporated this legislation into its national laws. However, it's worth noting that there are now distinctions in the terms and guidance provided by the UK since its departure from the EU. One notable difference pertains to adequacy decisions, where the EU and the UK hold varying viewpoints on countries that

[83] PDPL (n 40) Art. 68
[84] PDPL (n 40) Art. 70 (1)
[85] PDPL (n 40) Art. 70 (2)
[86] PDPL (n 40) Art. 71

align with their respective standards. In addition, the difference on the ‘safeguards’ established by the UK and the EU in the preceding section.

When comparing Indonesia to both the EU and the UK, it becomes evident that Article 56 of the Indonesian PDPL shares similarities with the concepts presented by the EU and the UK. Essentially, Indonesia permits data transfers as long as the recipient country offers equivalent legal protection, similar to the 'adequacy decisions' principle applied in this context. Next, even when the recipient country lacks standards equal to or surpassing the PDPL, the data controller must ensure suitable and legally binding protection for personal data. This can be achieved through contracts or other legally enforceable means, ensuring compliance with Indonesian law. In this case, the concept quite similar with the ‘appropriate safeguards’ owned by the EU and the UK. Nonetheless, Indonesia doesn't provide specific guidance on the format or interpretation of these contracts or agreements. In this regard, Indonesia could consider adopting interpretations from the legislation of the UK and/or EU to understand what should be incorporated into these contracts. Indonesia also embraces the concept of 'derogations,' applying them in a broader context, provided that the data subject gives consent to the data transfer. In other words, data can be transferred under specific circumstances as long as the individual whose data is being transferred agrees to it.

A notable distinction lies in the approach to sanctions: Indonesia opts for criminalizing data protection violations, whereas the EU and the UK primarily impose fines as penalties. In Indonesia, breaches of data protection can result in criminal charges, potentially leading to more severe legal consequences for individuals or entities found in violation, whereas the EU and the UK primarily rely on financial penalties to enforce compliance with data protection regulations.

D. Conclusion

The development of a legal framework for cross-border transfer of personal data is an ongoing process influenced by various factors, such as changes in technology, increasing global interconnectedness, and shifts in regulations and policies. Because of the proliferation of the internet and its fast growth, the movement of data has become both common and inevitable. Nonetheless, there is a significant potential for breaches of privacy when data is transferred. Therefore, in the majority of jurisdictions, international data transfer is restricted unless specific requirements stipulated by data protection law are met.

In the European Union, the GDPR stipulates three exceptions, namely adequacy decisions, appropriate safeguards, and derogations.

The same approach is also taken by the United Kingdom, which used the framework under the GDPR, although they produce several differences. The distinctive element concerns the adequacy decisions in which the United Kingdom tries to add more countries rather than the decision made by the EU and the new SCC that is issued by the UK ICOs. On the other hand, Indonesia, through its recent PDP Law, requires the data controllers that wish to transfer personal data must ensure that the receiving country has a level of protection that meets or exceeds the requirements of the PDPL. If this cannot be guaranteed, the organization must implement adequate measures to protect the data. If these options are not feasible, the organization must obtain consent from the individual whose data is being transferred before sending it overseas.

The authors believe that with the increasing reliance on cloud computing and the use of third-party service providers, the development of cross-border transfer of personal data is a complex and dynamic process that is likely to continue to evolve in response to changes in technology, global interconnectedness and shifts in regulations and policies. Indonesia, in this context, should specify safeguards related to contractual clauses that are permissible in cross-border transactions, drawing inspiration from the more detailed guidelines and practices established in the EU and the UK. It is essential for Indonesia to outline specific provisions and requirements concerning these contractual clauses to ensure clarity and consistency in cross-border data transfers, aligning its approach with the comprehensive frameworks in place within the EU and the UK.

References

Legislations

Indonesia Law No. 11 of 2008 on Information and Electronic Transactions.

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), OJ 2016 L 119/1 24.05.2016.

United Kingdom Data Protection Act (2018).

Indonesia Law No. 27 of 2022 on Personal Data Protection.

Books

ALLEA (European Federation of Academies of Sciences and Humanities), FEAM (Federation of European Academies of Medicine), and EASAC (European Academies' Science Advisory Council). *International Sharing of Personal Health Data for Research*. DE: ALLEA, 2021. https://doi.org/10.26356/IHDT.

Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd and updated ed. ed. Cambridge, Mass: MIT Press, 2006.

Bygrave, Lee A. *Data Privacy Law: An International Perspective*. 1st ed. Oxford, United Kingdom: Oxford University Press, 2014. https://academic.oup.com/idpl/article-abstract/5/1/88/622973.

Dumortier, Jos, Pieter Gryffroy, Ruben Roex, and Yung Shin van der Sype. *European Privacy and Data Protection Law*. Alphen aan den Rijn: Wolters Kluwer, 2022.

European Data Protection Board. *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018*. EDPB, 2018. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

European Union Agency for Fundamental Rights., Council of Europe (Strasbourg)., European Court of Human Rights., and European Data Protection Supervisor. *Handbook on European Data Protection Law: 2018 Edition.* LU: Publications Office, 2018. https://data.europa.eu/doi/10.2811/343461.

Greenleaf, G. W. *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. 1st ed. Oxford, United Kingdom ; New York, NY: Oxford University Press, 2014.

Hijmans, Hielke. *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. 1st ed. 2016. Issues in Privacy and Data Protection 31. Cham: Springer International Publishing : Imprint: Springer, 2016. https://doi.org/10.1007/978-3-319-34090-6.

Karo Karo, Rizky P.P., and Teguh Prasetyo. *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*. Bandung: Nusa Media, 2020.

Kuner, Christopher, Lee A Bygrave, Christopher Docksey, and Laura Drechsler, eds. *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University PressNew York, 2020. https://doi.org/10.1093/oso/9780198826491.001.0001.

Lloyd, Ian J. *Information Technology Law*. 9th ed. Oxford: Oxford University Press, 2020.

Mcgeveran, William. *Privacy and Data Protection Law*. 2nd ed. University Casebook Series. St. Paul: Foundation Press, 2023.

Millard, Christopher J. *Legal Protection of Computer Programs and Data*. Toronto : London: Carswell Co. ; Sweet & Maxwell, 1985.

Rücker, Daniel, and Tobias Kugler. *New European General Data Protection Regulation, a Practitioner's Guide: Ensuring Compliant Corporate Practice*. München Oxford Baden-Baden: C.H. Beck Hart publishing Nomos, 2018.

Taylor, Mark. *Genetic Data and the Law: A Critical Perspective on Privacy Protection*. 1st ed. Cambridge University Press, 2012. https://doi.org/10.1017/CBO9780511910128.

Ustaran, Eduardo, ed. *European Data Protection: Law and Practice*. Portsmouth, NH: an IAPP Publication, International Association of Privacy Professionals, 2018.

Voigt, Paul, and Axel Von Dem Bussche. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-57959-7.

Journals

Araújo, Alexandra Maria Rodrigues. "The Right to Data Protection and the Commissions' Adequacy Decision." *UNIO – EU Law Journal* 1 (July 1, 2015): 77–93. https://doi.org/10.21814/unio.1.6.

Birch, Kean, Dt Cochrane, and Callum Ward. "Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech." *Big Data & Society* 8, no. 1 (January 2021): 1–15. https://doi.org/10.1177/20539517211017308.

Casalini, Francesca, and Javier López González. "Trade and Cross-Border Data Flows." *OECD Trade Policy Papers*, OECD Trade Policy Papers, 279, no. 220 (January 23, 2019): 40. https://doi.org/10.1787/b2023a47-en.

Celeste, Edoardo. "Cross-Border Data Protection After Brexit." *SSRN Electronic Journal*, no. 4 (2021). https://doi.org/10.2139/ssrn.3784811.

Daigle, Brian, and Mahnaz Khan. "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." *Journal of International Commerce and Economics*, June 2020, 38. https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf.

Geradin, Damien, Dimitrios Katsifis, and Theano Karanikioti. "GDPR Myopia: How a Well-Intended Regulation Ended up Favoring Google in Ad Tech." *SSRN Electronic Journal*, 2020, 40. https://doi.org/10.2139/ssrn.3598130.

Hoofnagle, Chris Jay, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information & Communications Technology Law* 28, no. 1 (January 2, 2019): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

Jiménez-Gómez, Briseida Sofía. "Cross-Border Data Transfers Between the EU and the U.S.: A Transatlantic Dispute." *Santa Clara Journal of International Law*, 1, 19, no. 2 (May 1, 2021): 45. https://digitalcommons.law.scu.edu/scujil/vol19/iss2/1.

Lintvedt, Mona Naomi. "Putting a Price on Data Protection Infringement." *International Data Privacy Law* 12, no. 1 (March 18, 2022): 1–15. https://doi.org/10.1093/idpl/ipab024.

Newlands, Gemma, Christoph Lutz, Aurelia Tamò-Larrieux, Eduard Fosch Villaronga, Rehana Harasgama, and Gil Scheitlin. "Innovation under Pressure: Implications for Data Privacy during the Covid-19 Pandemic." *Big Data & Society* 7, no. 2 (July 2020): 14. https://doi.org/10.1177/2053951720976680.

Park, Jihyun and Heriyanto, Dodik Setiawan Nur. "In favor of an Immigration Data Protection Law in Indonesia and Its Utilization for Contract Tracing". *Prophetic Law Review* 4, no. 1 (2022). https://doi.org/10.20885/PLR.vol4.iss1.art1.

Stoilova, Veronika. "Regulation of International Data Transfers under EU Data Protection Law." *CES Working Papers* 13, no. 1 (2021): 16. https://ceswp.uaic.ro/articles/CESWP2021_XIII1_STO.pdf.

Sun, Yunchuan, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. "Data Security and Privacy in Cloud Computing." *International Journal of Distributed Sensor Networks* 10, no. 7 (July 1, 2014). https://doi.org/10.1155/2014/190903.

Vrbljanac, Danijela. "Personal Data Transfer to Third Countries – Disrupting the Even Flow?" *Athens Journal of Law* 4, no. 4 (September 30, 2018): 337–58. https://doi.org/10.30958/ajl.4-4-4.

Wolff, Josephine, and Nicole Atallah. "Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020." *Journal of Information Policy* 11 (December 1, 2021): 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063.

Yakovleva, Svetlana. "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities.'" *The Journal of World Investment & Trade* 21, no. 6 (September 11, 2020): 881–919. https://doi.org/10.1163/22119000-12340189.

Yuniarti, Siti. "PROTECTION OF INDONESIA'S PERSONAL DATA AFTER RATIFICATION OF PERSONAL DATA PROTECTION ACT." *Progressive Law Review* 4, no. 02 (November 23, 2022): 54–68. https://doi.org/10.36448/plr.v4i02.85.

Others

ALLEA. "Sharing Matters: Why International Data Transfer Is Crucial For Health Research." *ALLEA (European Federation of Academies of Sciences and Humanities)* (blog), April 26, 2021. https://allea.org/sharing-matters-why-international-data-transfer-is-crucial-for-health-research/.

Baig, Anas. "What To Know About The Russian Federal Law No. 152-FZ." securiti.ai, August 5, 2023. https://securiti.ai/russian-federal-law-no-152-fz/.

Chiavetta, Ryan. "UK Announces Independent Adequacy Decisions; Edwards Named ICO Top Candidate." iapp.org, August 26, 2021. https://iapp.org/news/a/uk-announces-independent-adequacy-decisions-edwards-named-ico-top-candidate/.

DA, Ady Thea. "Advokat Ini Ingatkan 3 Ketentuan Transfer Data Pribadi Ke Luar Negeri." *Hukumonline* (blog), October 4, 2022. https://www.hukumonline.com/berita/a/advokat-ini-ingatkan-3-ketentuan-transfer-data-pribadi-ke-luar-negeri-lt633baec525388/.

Deng, Jet Zhisong, and Ken Jianmin Dai. "China's Restrictions on Cross-Border Transfer of Personal Information: An Update on Regulatory Policy and Practical Implications." ibanet, February 17, 2023. https://www.ibanet.org/chinas-restrictions-on-cross-border-transfer-of-personal-information.

Department for International Trade and The Rt Hon Anne-Marie Trevelyan MP. "Digital Trade Key to Unlocking Opportunities of the Future." Press release. gov.uk, November 25, 2021. https://www.gov.uk/government/news/digital-trade-key-to-unlocking-opportunities-of-the-future.

Dorwart, Hunter, Katerina Demetzo, Dominic Paulger, Josh Lee Kok Thong, Lee Matheson, and Isabella Perera. "INDONESIA'S PERSONAL DATA PROTECTION BILL: OVERVIEW, KEY TAKEAWAYS, AND CONTEXT Indonesia's Personal Data Protection Bill: Overview, Key Takeaways, and Context." *Future of Privacy Forum* (blog), October 19, 2022. https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/.

General Data Protection Regulation (GDPR). "GDPR Third Countries." gdpr-info.eu, n.d. https://gdpr-info.eu/issues/third-countries/.

Global Data Alliance. "Cross-Border Data Transfers & Privacy." globaldataalliance.org, May 2020. https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf.

Hawkins, Andrew J. "Uber Admits Covering up Massive 2016 Data Breach in Settlement with US Prosecutors." theverge.com, July 25, 2022. https://www.theverge.com/2022/7/25/23277161/uber-2016-data-breach-settlement-cover-up.

Hubbard, Michael T. "Personal Data of U.S. Citizens Transferred Abroad Needs Protection." natlawreview, July 30, 2019. https://www.natlawreview.com/article/personal-data-us-citizens-transferred-abroad-needs-protection.

Information Commissioner's Office. "Guide to the General Data Protection Regulation (GDPR)." ico.org.uk, October 14, 2022. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

———. "International Data Transfers." ico.org.uk, n.d. https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/.

Kakadia, Keith. "A Comprehensive List of Social Media Statistics for Journalists." *Sociallyin* (blog), March 30, 2023. https://blog.sociallyin.com/social-media-statistics-for-journalists-by-sociallyin.

Klosek, Jacqueline. "Indonesia: A Long-Awaited Privacy Measure Finally Becomes Law In Indonesia." mondaq, November 16, 2022. https://www.mondaq.com/data-protection/1251262/a-long-awaited-privacy-measure-finally-becomes-law-in-indonesia.

Kurth, Hunton Andrews. "ICO Confirms UK Firms May Rely on Public Interest Derogation for SEC Transfers." natreview.com, January 29, 2021. https://www.natlawreview.com/article/ico-confirms-uk-firms-may-rely-public-interest-derogation-sec-transfers.

Lord, Nate. "What Is the Data Protection Directive? The Predecessor to the GDPR." digitalguardian.com, December 28, 2022. https://www.digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

Pisa, Michael, Pam Dixon, and Ugonma Nwankwo. "Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity." *Center for Global Development* (blog), August 11, 202AD. https://www.cgdev.org/publication/why-data-protection-matters-development-case-strengthening-inclusion-and.

Quixy Editorial Team. "80+ Eye-Opening Social Media Statistics for Every Channel." *Quixy.Com* (blog), August 2023. https://quixy.com/blog/social-media-statistics-for-every-channel/.

Sayce, David. "The Number of Tweets per Day in 2022." Personal blog. *Dsayce.Com* (blog), 2022. https://www.dsayce.com/social-media/tweets-day/.

Shvartsman, Daniel. "Facebook: The Leading Social Platform of Our Times." investing.com, August 2023. https://www.investing.com/academy/statistics/facebook-meta-facts/.

Thea DA, Ady. "Advokat Ini Ingatkan 3 Ketentuan Transfer Data Pribadi Ke Luar Negeri." hukumonline, October 4, 2022. https://www.hukumonline.com/berita/a/advokat-ini-ingatkan-3-ketentuan-transfer-data-pribadi-ke-luar-negeri-lt633baec525388/.

"UK Approach to International Data Transfers," August 26, 2021. https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers.

UNCTAD. "Data Protection Regulations and International Data Flows: Implications for Trade and Development." unctad.org, April 2016. https://unctad.org/publication/data-protection-regulations-and-international-data-flows-implications-trade-and.

Wijaya, Glenn. "Residual Issues in Indonesia's Forthcoming Personal Data Protection Law." iapp.org, August 18, 2022. https://iapp.org/news/a/residual-issues-in-indonesias-forthcoming-personal-data-protection-law/.

Others

CJEU - C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559

Dumortier, Jos, and Caroline Goemans. "Data Privacy and Standardization." Discussion Paper presented at the CEN/ISSS Open Seminar on Data Protection, Brussels, March 23, 2000. https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/90cen-paper2f90.pdf.