Indonesian Journal of International Law

Volume 20 | Number 3 Article 2

April 2023

Competent Forum and Applicable Law in Personal Data Protection with a Foreign Element

Muhammad Faqih Adhiwisaksana
Universitas Indonesia

Tiurma Mangihut Pitta Allagan
Universitas Indonesia, tiurma@ui.ac.id

Indonesian Journal of International Law (2023), Vol. 20 No. 3, pp. 349 - 378
http://doi.org/10.17304/ijil.vol20.3.2

THE COMPETENT FORUM AND THE APPLICABLE LAW IN PERSONAL DATA PROTECTION WITH FOREIGN ELEMENT

Muhammad Faqih Adhiwisaksana*, Tiurma M. Pitta Allagan*

* Faculty of Law, Universitas Indonesia, Indonesia
Correspondence: tiurma@ui.ac.id

Abstract

This research analyses on personal data protection with a foreign element as a private international law issue, focusing on competent forum and applicable law. The author uses a juridical-normative research method with literature studies to explain the relevant private international law principles, as well as Indonesian laws and regulations surrounding competent forum and applicable law regarding competent forum and applicable law on personal data protection with a foreign element. The study found that various private international law principles may be used to determine the applicable law in personal data protection with a foreign element dispute, such as nationality, place where the tort occurred, or center of gravity. Indonesian courts are also competent to examine personal data protection with a foreign element case under Indonesian law. This study also elaborates practical implementation personal data protection with a foreign element, in particular on the competent forum and applicable law, as shown in the businesses Intercompany Agreement on Data Processing by X group company and in a cross-border acquisition transaction.

Keywords: *applicable law; competent forum; personal data protection; Indonesian private international law.*

I. INTRODUCTION

The principles of Private International Law ("**PIL**") should be applicable to determine the competent forum and applicable law in personal data protection with a foreign element. Data protection appears on the internet, which is a unique medium, are no different from the real world. The protection could cross the territory of the states and therefore allowing the application of existing PIL principles in determining the choice of law and the choice of forum as the classic scope of PIL.

The internet is one of the most important innovations of the 21st century. Through the internet, humans can access a wide variety of information, communicate instantly, as well as transact with partners located in different countries or continents. This enables a

variety of innovations in many areas such as commerce and business (*e-commerce*), transportation, tourism, government (*e-government*), finance, health, as well as completely new innovations such as social media, smartphones, and cloud computing.[1] There are currently more than 4.95 billion internet users in the world, which makes up 62.5 percent of the world's population.[2] Of these, 202.6 million people come from Indonesia, with an internet penetration rate of 73.7 percent. [3] As a network of computers connected through telecommunications facilities, the internet pays no particular attention to the physical location of the computers that transmit or receive information. The Internet also lacks centralized storage locations, control points, or communication lines. This makes communication on the internet virtual or separate from physical elements and geographical locations.[4] At the same time, the Internet is also ubiquitous, in which information can be transmitted throughout the world instantly and in which legal relations can occur between the parties without any other physical element apart from the parties themselves.[5]

In communicating, transacting, or doing activities on the internet, users may be asked to provide their personal data, which is then processed by another party which provides the services offered on the internet. The virtual nature of the internet allows personal data from one country, to be collected and processed by other parties located in another country. This is certainly very relevant for Indonesia, where eight of the ten most frequently accessed sites in Indonesia are sites operated by parties domiciled outside Indonesia.[6] Seeing that personal data can identify its owner specifically, the protection of personal

---

[1] Dewa Gede Sudika Mangku, *et al*., "The Personal Data Protection of Internet Users in Indonesia", *Journal of Southwest Jiaotong University* 56 (2021): 203.

[2] "Digital 2022: Global Overview Report", Data Reportal, accessed 7 February 2022, https://datareportal.com/reports/digital-2022-global-overview-report.

[3] "Digital 2021: Indonesia", Data Reportal, accessed 7 February 2022, https://datareportal.com/reports/digital-2021-indonesia.

[4] Edina Marton, *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law* (Nomos, 2016), 56.

[5] Oren Bigos, "Jurisdiction over Cross-Border Wrongs on the Internet", *The International and Comparative Law Quarterly* 54 (2005): 588-590.

[6] "Most Visited Websites by Traffic in Indonesia for all categories, June 2022", Semrush, accessed 8 February 2022, https://www.semrush.com/website/top/indonesia/all/.

data of internet users, or more commonly referred to as personal data protection, is important. In particular, the ubiquitous and virtual nature of the internet shows the importance of personal data protection with a foreign element, namely the protection of personal data belonging to a data subject (i.e., the person from which the data originates) from one country which is processed in another country. Prior to determining how the laws and regulations of a particular country carry out personal data protection with a foreign element, a more principal question is of course which country's law apply in such personal data protection with a foreign element, and in the case of dispute, which country's forum would be competent. These two questions are the most pivotal PIL question that arises in a personal data protection with a foreign element.[7] The importance arises because the virtual and ubiquitous nature of the internet itself allows the information to be spread to various countries immediately that end to various connecting points in various countries.

Considering the above, this study discusses the development of laws and regulations on personal data protection in Indonesia, in particular the personal data protection ("PDP") with a foreign element. The author also discusses the PIL aspects in PDP with a foreign element, especially regarding the competent forums and applicable law, both in theory and in practical questions.

The research method of this article is juridical-normative, of a descriptive nature, qualitative and descriptive analytical.[8] The research is based on library materials and secondary data that includes primary legal materials (the PDP Law), secondary legal materials (the relevant books and current journals).[9]

The outline of this article consists of the introduction, relevant PIL principles and provisions; PDP development and in Indonesia; case studies; and conclusion respectively.

---

[7] Tobias Lutzi, "Internet Cases in EU Private International Law-Developing A Coherent Approach", *International and Comparative Law Quarterly* 66 (2017): 690.
[8] *Ibid*., 96.
[9] Soerjono Soekanto, *Pengantar Penelitian Hukum [Introduction to Legal Research]*, (Jakarta:UI-Press, 2015), 52.

II. THE PIL PRINCIPLES IN RELATION TO PDP WITH FOREIGN ELEMENT

A. IN DETERMINING APPLICABLE LAW

Before determining which forum is competent and which law is applicable in a PDP with a foreign element, it is necessary to first identify whether a case is a case of Private International Law ("**PIL**") or not. It can be done by looking at the presence or absence of Primary Connection Points ("**PCP**") which are the things and circumstances that constitutes a PIL relationship. The relevant PCPs in a PDP matter are: (i) nationality; (ii) domicile; (iii) residence; (iv) legal seat in the case of a legal entity; and (v) choice of law in a contract.[10] After identifying whether an issue is an PIL issue or not, the next step is to determine what law applies. This can be done by identifying a Secondary Connection Point ("**SCP**") that will be used by the judge to determine what law applies in examining a PIL case. In case of PDP, the following SCP may be used to determine the applicable law:

1. Nationality;[11] Nationality of the data subject may be used to determine what law applies in a case of PDP with a foreign element. Law of the nationality of the data subject also determines whether the data subject has the legal capacity to carry out a legal action related to its personal data.
2. Domicile;[12] the domicile of the data subject may also be used to determine which law applies in a case of PDP with a foreign element, in particular if the nationality of a data subject is unable to be determined.
3. Residence;[13] the residence of the data subject may be used to determine which law to be governed in a case of PDP with a foreign element, in particular if the domicile of the data subject is yet to be formed.

---

[10] Sudargo Gautama, *Pengantar Hukum Perdata International Indonesia [Introduction to Indonesian Private International Law],* (Jakarta: Binacipta, 1987), 26-42.
[11] *Ibid*, 26.
[12] *Ibid.,* 31.
[13] *Ibid*., 33.

4. The legal seat in the case of a legal entity;[14] the legal seat of a legal entity may be used to determine which law applies in a case of PDP with a foreign element. This is especially relevant for PDP Controllers and Personal Data Processors, which are usually in the form of a legal entity. Similar to the nationality onto a natural person, the legal seat of a legal entity determines the legal capacity of said legal entity to carry out any legal action. There are various approaches to determine where is the legal seat of a legal entity is located, such as where the center of administration of the legal entity is located, or where the legal entity is incorporated. In case of Indonesia, Indonesian law determines that the law applicable to determine the personal status of a legal entity is the law where said legal entity is incorporated and headquartered in.
5. The place where tort occurs (*Lex Loci Delicti Commisie*);[15] In the event a tort occurs regarding PDP with a foreign element, the law of the place where the tort occurs may be used to examine the tort case. However, considering the virtual and ubiquitous nature of the internet, this may result in multiple countries having a SCP to the case. This may happen in the event of a personal data breach, where a personal data of a data subject is illegally accessed and made available around the world.
6. The choice of law,[16] the place where the agreement is made (*Lex Loci Contractus*) and the place where the legal action is carried out (*Lex Loci Executionis*);[17] these are SCP in relation with the contracts. The choice of law between parties in a processing of personal data with a foreign element will determine what law applies to the PDP with a foreign element. In the absence of a choice of law (whether explicit or implicit), the law of place where the legal action is carried out (e.g. where the processing of the data subject's personal data will be carried out) or where the agreement is made may be used instead. However, considering

[14] *Ibid*., 34.
[15] *Ibid*., 42.
[16] *Ibid.,* 34.
[17] *Ibid.,* 41-42.

that the data subject's personal data may be processed in more than one country, more than one country's law may be applicable in the case. Furthermore, considering the virtual nature of internet, it may be difficult to conclusively determine where the agreement takes place, whether on the data subject's location, or where the personal data controller is legally seated, or where the data server is located.

7. The center of gravity.[18] According to the center of gravity doctrine, the law of the place that has the most important connection to the case shall be applied. In the case of personal PDR with a foreign element, it can be understood that the most important aspect to be considered is the protection of the data subject's right to its personal data. Therefore, under this theory, each connection shall be counted and the law that has most connection shall be the applicable law.

B. PIL PRINCIPLES IN DETERMINING COMPETENT FORUM

In Indonesia, the following provision of Indonesian laws and regulations stipulate that Indonesian courts are competent to examine cases of PDP with a foreign element:

1. Article 118 of the Het Herzeiene Indonesisch Reglement ("HIR")

   The HIR is the procedural law for civil cases that applies to Java and Madura islands in Indonesia. Article 118 of the HIR stipulates that Indonesian courts is competent to adjudicate civil or commercial cases if the defendant is domiciled or having legal domicile within the jurisdiction of a district court[19] or within the jurisdiction of other district court in Indonesia that have been specifically and expressly agreed by the parties in their contract.[20] This means that a foreign data subject may file a suit against an Indonesian personal data controller or personal data processor in an Indonesian district court which has jurisdiction over the Indonesian personal data controller's

[18] Hugh S. McManus, "Conflict of Laws: The "Center of Gravity" Theory Applied to Torts: Babcock v. Jackson", *Marquette Law Review* 47 (1963), 255-256.
[19] Art.118 HIR, para. 1.
[20] Art.118 HIR, para. 4.

or personal data processor's domicile, or in an Indonesian district court that has been specifically and expressly agreed by the parties in their contract, and either Indonesian district court will be competent to examine the case.

2. Article 100 of the Reglement op de Burgerlijke Rechtsvordering ("**RV**")

   The RV is the procedural law for civil cases that is applicable for Europeans and Orientals (also known as *Vreemde Oosterlingen*, a category of people from non-European countries but not Indonesia, such as Arab countries, China, India, and others). During the Dutch colonization period, where Indonesia is known as Dutch East Indies, Article 131 of the *Indische Staatsregeling* ("**IS**"), the Dutch East Indies government constitution, divided Indonesian resident into three groups: (i) Europeans; (ii) Natives or *Bumiputera*; and (iii) Orientals. However, with the issuance of Ampera Cabinet Presidium Decree No. 31/U/IN/12/1966 after Indonesian independence, such grouping has been revoked and the RV now applies to all Indonesian citizens.

   Article 100 of the RV stipulates that Indonesian citizens may file a suit against foreign citizens, that are not an Indonesian resident, in an Indonesian district court for agreement executed anywhere. This means that an Indonesia citizen which is a data subject may file a suit against foreign Personal Data Controller or Personal Data Processor in an Indonesian district court, and such Indonesian district court will be competent to examine the case.

3. Article 3 of the Algemene Bepalingen van Wetgeving voor Indonesie ("**AB**")

   The AB is a law that stipulates general provisions regarding Indonesian laws and regulations. Article 3 of the AB stipulates that unless determined otherwise, civil law and commercial law for Indonesian citizens also apply for foreigners.

   It is important to note that despite the HIR, RV, and AB being promulgated by the Dutch East Indies Government, Article I of the Transitionary Provisions of the Indonesian Constitution stipulates that all existing laws and regulations that already exist are still in

force prior to the formulation of a new one under the Indonesian Constitution. Therefore, Indonesian courts have jurisdiction to examine any dispute of personal data protection with a foreign element.

In relation to the procedural law, the procedural law in examining a PDP with a foreign element dispute in Indonesia shall be the Indonesian law civil procedural law. This is in line with the PIL principles whereby the forum (whether the court, arbitral tribunal, or government institution) will use the procedural law applicable where the legal proceeding is initiated.[21]

III. PDP DEVELOPMENT IN INDONESIA

A. THE CONCEPT OF PDP AND ITS DEVELOPMENT

Personal data consist of information regarding individuals and their behavior or data that can identify a living individual.[22] The data can be in the form of name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person.[23] As data that can identify a specific individual, personal data is closely related to privacy. Naturally, humans always need privacy. According to Alan Westin, there are four functions of privacy that are relevant to humans. The first is to fulfill the need for personal autonomy to favor normal psychological functioning, stable human relations, and self-development. The second is as a form of emotional release. Privacy supports healthy psychological functioning by providing an opportunity for the body to rest and vent feelings without fear. The third is for self-evaluation and decision making, where the opportunity of self-

---

[21] Zulfa Joko Basuki, *et al*., *Hukum Perdata Internasional [Private International Law]*. (Universitas Terbuka, 2014), 20.

[22] Arno R. Lodder, "Internet Law", in *The SAGE Encyclopedia of the Internet vol. 2*, Barney Warf, ed. (Sage Publications Ltd., 2018), 521.

[23] European Union, Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, Art. 4 (1).

reflection can give time to process the existing information in order to be able to take appropriate steps. The fourth function is to meet the need for a limited and protected communication, for example with family, friends, or closest co-workers. [24] Therefore, the protection of individual privacy is one of the important human rights to be protected, including the protection of personal data as a form of privacy protection.

The global development of personal data protection can be seen through several milestones. The German state of Hesse enacted the first law on privacy protection in the form of the Data Protection Act in 1971. Further international developments happened through the Universal Declaration of Human Rights ("**UDHR**") of the United Nations ("**UN**") adopted on 10 December 1948. Article 12 of the UDHR provides protection to the privacy of the communications and personal territory of any person such as the family, and states that no one can be arbitrarily interfered with in his privacy, his family, his household, or correspondence, as well as against violations of his honor or reputation. Article 12 of the UDHR also states that everyone is entitled to legal protection against such interference or violation. Although as a resolution of the UN General Assembly the UDHR is not legally binding, the UDHR is the first international instrument to recognize and protect the right to privacy. Later, Article 12 of the UDHR was restated in Article 17 of the International Covenant on Civil and Political Rights ("**ICCPR**"), an international treaty that took effect on 23 March 1976 and ratified by Indonesia through Law Number 12 of 2005 on the ratification of the International Covenant on Civil and Political Rights.

Further developments occurred in 1950, when the European Convention for the Protection of Human Rights and Fundamental Freedoms ("**ECHR**") was formulated by the Council of Europe. The ECHR became the world's first binding legally binding legal instrument that protects the right to privacy and divides it into three parts: the privacy of personal and family life, the privacy of the place of residence, and the privacy of correspondence limited to the confidentiality of letters. Even so, the ECHR also provides that the right to privacy is not absolute

[24] Alan Westin, *Privacy and Freedom* (The Bodley Head, 1967), 330-338.

and allows for the intrusion of public authority if it is required under the law and needed in a democratic society for certain interests, such as security. The ECHR also has a legal mechanism for its enforcement through the European Commission and must be effective in the laws of the country that ratified it.[25]

In 1981 the first convention specifically regulating the processing of personal data was formulated by the Council of Europe, namely the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("**CPIRAPPD**"). The Convention was formulated on 28 January 1981, and entered into force on 1 October 1985. Broadly speaking, this convention provides general guidance regarding the automated processing of data in the public and private sectors such as regarding data quality, protection of data in certain categories such as race, personal data security, additional protection for data subjects, and cross-border data flows.[26] What is interesting about this convention is that although it was created by the Council of Europe, there are several non-European countries that have also ratified this convention, including Argentina, Tunisia, and Mauritius.[27]

In the formulation of the CPIRAPPD, the Council of Europe applied the principles of personal data protection formulated by the Organisation for Economic Co-operation and Development ("**OECD**") in 1980 in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("**OECD Guidelines on the Protection of Privacy"**). The OECD also says that the protection of personal data is a form of privacy protection. The data protection principles put forward by the OECD are as follows:[28]

---

[25] J. Holvast, "The Protection of Privacy" in the *The History of Information Security: A Comprehensive Handbook*, Karl de Leeuw and Jan Bergstra, eds. (Elsevier Science, 2007), 752.

[26] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe Treaty Series No. 108 (1981), Chapter II.

[27] "Chart of Signatures and Ratifications of Treaty 108" Council of Europe, accessed 18 April 2022, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108, accessed April 18, 2022.

[28] Organisation for Economic Co-Operation and Development, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, Part Two.

1. Collection Limitation Principle. This principle states that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle. This principle states that the personal data collected should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.
3. Purpose Specification Principle. This principle states that the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle. This principle states that personal data must not be disclosed, made available or otherwise used for purposes other than the purpose specifically stated except: (1) with the consent of the data subject; or (2) by the authority of law.
5. Security Safeguards Principle. This principle states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness Principle. This principle states that should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle. This principle states that an individual must have the right to:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a

reasonable manner; and in a form that is readily intelligible to him;

c. to be given reasons if a request made under letter (a) and (b) is denied, and to be able to challenge such denial;

d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle. This principle states that the data controller should be accountable for complying with measures which give effect to the principles stated above.

The existence of the CPIRAPPD and the OECD Guidelines on the Protection of Privacy still leaves obstacles for the member states of the European Union ("**EU**") because of different application of the principles of the OECD Guidelines on the Protection of Privacy in each EU member state. Therefore, in 1995 the EU took steps to harmonize the rules within the EU through Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regarding the processing of personal data and on the free movement of such data ("**EDPD**"). As a directive, the EDPD is a legislative law that defines the goals that all EU member states must achieve, where each EU member state has the freedom to apply its own state regulations to achieve this goal. [29] The EDPD applies to both the public and private sectors and regulates the processing of personal data in a manual and automated manner. The EDPD also provides more clearly how the principles of the OECD Guidelines on the Protection of Privacy are applied in practice, particularly regarding data quality and the criteria for ensuring that data processing is lawful, the terms of data processing of certain categories or criminally related, as well as the rights of data subjects and the obligations of data controllers. The EDPD also requires EU member states to have public authorities overseeing the implementation of the EDPD and restricts the transfer of personal data to countries that are not EU members.[30]

---

[29] "Types of Legislation," European Union, accessed 18 April 2022, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en, accessed April 18, 2022.

[30] J. Holvast, "The Protection of Privacy", 754.

Although the EU has implemented EDPD, it has not succeeded in harmonizing the personal data protection within the EU, due to differences in regulations issued by each EU member state. Certain data processing activities permitted by one of the EU member states may be prohibited by other EU member states. To rectify this issue, in 2016 the EU adopted Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"). As a regulation, the GDPR is a law that is binding on all EU member states and must be implemented thoroughly.[31] This resulted in the same personal data protection rules in EU member states, increasing legal certainty and increasing EU citizens' confidence in the responsible treatment of their personal data. The GDPR is currently one of the most complete regulations regarding the protection of personal data and is an inspiration for countries other than EU members to also formulate their personal data protection regulations, including Indonesia.

B. PDP IN INDONESIAN LAWS AND REGULATIONS

Firstly, under Article 499 of the Indonesian Civil Code ("**ICC**"), personal data is considered as rights which can be the subject of property rights, therefore it is considered as an asset.[32] Currently, PDP regulation in Indonesia is spread among a variety of different laws and regulations which are all effective and applicable. These includes Law Number 11 of 2008 on the Electronic Information and Transactions as amended by Law No. 19 of 2016 ("**EIT Law**"), Regulation of the Minister of Communication and Informatics Number 20 of 2016 on the Personal Data Protection in Electronic Systems ("**MoCI Reg. 20/2016** "), Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions ("**GR 71/2019**"), and Government Regulation Number 80 of 2019 on the Trade through Electronic Systems ("**GR 80/2019**"). Indonesia has also recently passed the Law No. 27 of

[31] European Union, "Types of Legislation."
[32] Indonesia, *Burgerlijk Wetboek* (*Civil Code*), translated by Prof. R. Subekti, S.H. and R. Tjitrosudibio (2017, Balai Pustaka), Art. 499.

2022 on the Personal Data Protection ("**PDP Law**"). In this article, the author will focus on the PDP Law.

The PDP Law has been in force since 17 October 2022. The PDP Law defines personal data (henceforth, "**Personal Data**") as "any data about an individual whether identified and/or identifiable individually or combined with other information either directly or indirectly through electronic and/or non-electronic systems." [33] Furthermore, the PDP Law also defines personal data subject (henceforth, "the **Subject**") as, "individuals to whom Personal Data is attached."[34] The PDP Law also defines personal data controller (henceforth, "the **Controller**") as, "every person, public agency, and international organization that acts individually or jointly in determining purposes and exercising control over the processing of Personal Data."[35] Another role that the PDP Law defines is the personal data processor (henceforth, "the **Processor**"), defined as, "every person, public agency, and international organization that act individually or jointly in Personal Data processing on behalf of a Personal Data Controller."[36]

The PDP Law applies to any person (whether natural person or corporation), public agency,[37] and international organization[38] that performs legal actions regulated by the PDP Law which is: (a) located within the jurisdiction of Indonesia; or (b) outside the jurisdiction of

---

[33] Indonesia. *Undang-Undang tentang Perlindungan Data Pribadi*. UU No. 27 Tahun 2022. (*Personal Data Protection Law*. Law No. 27 of 2022). Art. 1 No. 1.
[34] *Ibid*. Art. 1 No. 6.
[35] *Ibid*. Art. 1 No. 4.
[36] *Ibid*. Art. 1 No. 5.
[37] The PDP Law defines Public Agency as "an executive, a legislative, a judicial, and other agencies whose main functions and duties are related to the administration of the state, whose funds are partially or entirely sourced from the State Revenue and Expenditure Budget and/or Regional Revenue and Expenditure Budgets, or non-governmental organizations insofar that part or entire funds are sourced from the State Revenue and Expenditure Budget and/or Regional Revenue and Expenditure Budgets, public and/or overseas donations."
[38] The PDP Law defines International Organization as "an organization that is recognized as a subject of international law and has the capacity to create an international agreement."

Indonesia which has legal consequences in the jurisdiction of Indonesia and/or for Indonesian Citizens outside the jurisdiction of Indonesia.[39]

The PDP Law distinguishes Personal Data into two types. The first is general Personal Data, which includes: full name; gender; citizenship; religion; and/or Personal Data combined to identify an individual (e.g., a combination of Internet Protocol address and cell phone number to identify a particular individual). The second is specific Personal Data, which includes: health data and information; biometric data; genetic data; crime records; children's data; personal financial data; and/or other data in accordance with the provisions of laws and regulations. [40] Some examples of "other data in accordance with the provisions of laws and regulations" are medical records and immigration prevention list.

Broadly speaking, the Subject has several rights protected in the PDP Law, namely:[41]

1. The right to request information about clarity of identity, the basis of legal interest, the purpose of the request and use of Personal Data, and the accountability of the party requesting the Personal Data.
2. The right to complete, update and/or correct errors and/or inaccuracies in Personal Data about them in accordance with the purposes for which the Personal Data was processed.
3. The right to access and obtain a copy of their Personal Data in accordance with the provisions of laws and regulations.
4. The right to terminate the processing, deletion and/or destruction of Personal Data about themselves in accordance with the provisions of laws and regulations.
5. The right to withdraw consent to the processing of Personal Data about themselves that has been granted to the Controller.
6. The right to object to decision-making actions based solely on automated processing, including profiling, that gives rise to legal

[39] Personal Data Protection Law. Art. 2.
[40] *Ibid*. Art. 3.
[41] *Ibid*. Art. 5-14.

consequences or has a significant impact on the Personal Data Subject.

7. The right to delay or restrict the processing of Personal Data in proportion to the purposes for which the personal data was processed.
8. The right to sue and receive compensation for the breach of his Personal Data in accordance with the provisions of laws and regulations.
9. The right to obtain and/or use its Personal Data from the Controller in a form that is in accordance with the structure and/or format commonly used or readable by electronic systems or hardware used in interoperability between electronic systems.
10. The right to use and transmit their own Personal Data to other Controllers, as long as the system can communicate with each other securely in accordance with the principles of Personal Data protection under the PDP Law.

It is important to note, however, that the above Personal Data Subject's rights no. 4-7 and no. 9-10 are excluded for:

1. the interest of national defense and security;
2. the interest of law enforcement process;
3. public interest in the context of state administration;
4. the interest of supervision of the sectors of financial services, monetary, payment system, and financial system stability carried out in the context of state administration; or
5. the interest of statistics and scientific research.

The above shall be implemented solely in the context of implementing the provisions of the PDP Law.[42]

In the PDP Law, the processing of Personal Data (henceforth, "**Processing**") includes acquisition and collection; processing and analysis; retention; rectification and updating; display, announcement,

[42] *Ibid*. Art. 15.

transfer, dissemination, or disclosure; and/or deletion or destruction.[43] The processing of such Personal Data shall be carried out in accordance with the principles of personal data protection as follows:[44]

1. carried out in a limited and specific manner, legally valid, appropriate, and transparent.
2. carried out in accordance with its purpose.
3. carried out by guaranteeing the rights of the Subject;
4. carried out accurately, completely, not misleading, up-to-date, and accountable.
5. carried out by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of Personal Data.
6. carried out by notifying the purposes and activities of the processing, as well as the failure to protect Personal Data.
7. Personal Data shall be destroyed and/or deleted after the retention period ends or at the request of the Data Subject unless otherwise provided by laws and regulations; and
8. carried out responsibly by fulfilling the implementation of the principles of personal data protection and can be clearly proven.

1. Under the PDP Law, the processing of personal data must have the following Personal Data processing basis:[45]explicit consent of the Subject for 1 (one) or several specific purposes that have been submitted by the Controller to the Subject, for which the Controller shall include information on:[46]

   a. the legality of the Personal Data Processing;
   b. the purpose of the Personal Data Processing;
   c. types and relevancy of Personal Data to be Processed;
   d. retention period of documents containing Personal Data;
   e. details of the information gathered;

[43] *Ibid*. Art. 16 para. (1).
[44] *Ibid*. Art. 16 para. (2).
[45] *Ibid*. Art. 20.
[46] *Ibid*. Art. 21 para. (1).

f. Personal Data Processing period; and
g. Subject's rights.

2. fulfillment of the obligations of the agreement in the event that the Subject is one of the parties or to fulfill the request of the Subject at the time of entering into the agreement.
3. fulfillment of the legal obligations of the Controller in accordance with the provisions of laws and regulations.
4. fulfillment of the protection of the vital interest of the Subject.
5. exercise of the authority of the Controller in accordance with the provisions of laws and regulations.
6. fulfillment of the obligations of the Controller in public services for the public interest; and/or
7. fulfillment of other legitimate interests by taking into account the purposes, needs and balance of interests of the Controller and the rights of Subject.

The PDP Law also further stipulates the provisions regarding the consent from the Subject. Consent given by the Subject must be in writing or recorded either electronically or non-electronically. Furthermore, if written consent contains other purposes, the request for consent must meet the conditions as follows, in a form of a clearly distinguishable from other matters; made in a format that is understandable and accessible; and uses simple and clear language. If this is not fulfilled, then the consent is declared null and void.[47]

The PDP Law stipulates the following provisions on Personal Data transfer [48] carried out by Controllers from within the jurisdiction of Indonesia to Controllers and/or Processors outside the jurisdiction of Indonesia. Prior to carrying out the Personal Data transfer to outside Indonesian jurisdiction,[49] it is important to note that under the PDP Law, the Indonesian PDP Institution (as defined below) will be authorized

[47] *Ibid*., Art. 22 and 23.
[48] The PDP Law defines Personal Data transfer as the "is the displacement, delivery, and/or duplication of Personal Data from the Controller to a third party whether electronically or non-electronically".
[49] Indonesia, *PDP Law*, Art. 56 paragraphs (2) – (4).

to carry out assessment towards the fulfillment of requirements for Personal Data transfer to outside the jurisdiction of Indonesia, which may include stipulating adequacy decision stating that a country has an equivalent or higher level of personal data protection than what is stipulated in the PDP Law. With that in mind, it is best for Controller who intends to carry out Personal Data transfer to outside the jurisdiction of Indonesia to ensure that there is an adequate and binding personal data protection or to obtain consent from the Subject.

The PDP Law also regulates the state institution that shall carry out the implementation of personal data protection (henceforth, "the **Indonesian PDP Institution**"). The Indonesian PDP Institution is appointed by and accountable to the president of Indonesia and is tasked with:[50]

1. the formulation and establishment of personal data protection policies and strategies that serve as guidelines for Subjects, Controllers, and Processors;
2. the supervision of the implementation of the personal data protection;
3. the enforcement of administrative laws against violations of the PDP Law; and
4. the facilitation of out-of-court dispute resolution.

The PDP Law also provides administrative sanctions for violations of certain provisions in the PDP Law, including regarding the transfer of personal data outside the jurisdiction of Indonesia. Administrative sanctions that may be imposed are: written warnings; temporary cessation of personal data processing activities; erasure or destruction of personal data; indemnity; and/or administrative fines.[51]

In view of the PDP Law together with the PIL principles, the PDP Law applies to any person, public agency, and international organization, including to Controllers and Processors located outside the jurisdiction of Indonesia which activities has legal consequences in the jurisdiction of Indonesia and/or for Indonesian Citizens outside the jurisdiction of

[50] *Ibid*., Art. 58 and Art. 59.
[51] *Ibid*., Art. 57 paragraphs (1) and (2).

Indonesia who are Subjects. Indonesian courts will have jurisdiction to examine personal data protection with a foreign element case in the event of the following:

1. in cases where the defendant is domiciled or having legal domicile within the jurisdiction of a district court in Indonesia. For example, in cases where an Indonesian Controller or Processor is being sued by a foreign Subject, said Subject may file a suit in a district court in Indonesia with jurisdiction over the defendant's domicile or legal domicile.
2. in cases where the parties in a Personal Data Processing agreement agree to choose a district court in Indonesia as the competent forum to resolve their dispute.
3. in cases where an Indonesian citizen file a suit against a foreign citizen that are not an Indonesian resident for agreements executed anywhere, including outside Indonesia. As an example, an Indonesian Subject may file a suit against a foreign Controller or Processor for failure to protect its data in a district court in Indonesia.

In such personal data protection with a foreign element dispute that is filed to an Indonesian court, if the personal data that is involved belongs to an Indonesian citizen, then the court may decide that the Indonesian law shall apply, by application of the center of gravity doctrine seeing that the Indonesian law has the most significant relationship to the event, being the protection of Indonesian citizen as data subjects.

IV. CASE STUDIES

A. INTERCOMPANY AGREEMENT ON DATA PROCESSING

Since the promulgation of the PDP Law, Indonesia has yet to have a personal data protection with a foreign element dispute in Indonesian courts. In light of this, this sub chapter will elaborate on a Personal Data Processing agreement and an imaginative case whereby the PIL principles apply in a personal data protection case.

To start, the author have examined an Intercompany Agreement on Data Processing ("**Intercompany Agreement**"), which is a contract made by and between all companies that are members of X group (henceforth, "**X Group**"), an international group of companies which has group companies operating in Indonesia (henceforth, members of X group shall be referred to as "**X Group Company**" and the company operating in Indonesia which is a member of X group company shall be referred to as "**PT X Indonesia"**). The description of the Intercompany Agreement is obtained from an interview with a member of PT X Indonesia's legal department. The fact that the signatories of this Intercompany Agreement are companies from different countries, each subject to the laws of their country, makes this Intercompany Agreement a PIL agreement.

The participation of a X Group Company to the Intercompany Agreement is carried out by way of executing a declaration of accession to the Intercompany Agreement, from which a list of X Group Companies that have acceded to the Intercompany Agreement is made available on X Group's internal website. This Intercompany Agreement sets outs the rights and obligations of all parties involved in the processing of personal data in any service relationship governed by this Intercompany Agreement, taking into account the requirements of applicable data protection law. This Intercompany Agreement will apply when personal data is processed under the terms of a service description, in which the service provider will act as a personal data processor to the service recipient. In processing said personal data, the personal data processor is obligated to carry out data processing in accordance with applicable data protection law and Article 5 (*purpose of the collecting, processing and use; type and content of data*), Article 6 (*technical and organizational measures*), Article 7 (*compliance with data secrecy by employees*), Article 13 (*Joint Controller Agreements*), Article 14 (*Term and termination*), and Article 15 (*Miscellaneous*) of the Intercompany Agreement.

The Intercompany Agreement also sets out provisions regarding restricted transfers, which is defined as any processing (including transfers and onwards transfers) of personal data originating from a personal data controller located within the European Economic Area

(henceforth, "**EEA**"), a country with an Adequacy Decision[52] (excluding Canada), or a country with similar adequacy requirements as contained in Article 35 *et seq*. of the GDPR[53] (such as the United Kingdom and Switzerland) by a service provider or any of its sub-processors outside the EEA and outside a country with an Adequacy Decision (henceforth, the restricted transfer shall be referred to as "**Restricted Transfer**"). Under Article 4 (*Restricted Transfers*), in the event of a Restricted Transfer, such activity shall be protected by adequate transfer safeguards in the form of an Adequacy Decision or appropriate safeguards as required by Article 46 of the GDPR as follows:

1. if and to the extent the parties enter into a service description and the personal data controller for the personal data that is processed is a X Group Company or a personal data controller that is otherwise bound by X Group binding corporate rules, the transfer safeguard applicable to the processing operations provided by the service provider is the X Group binding corporate rules, and the transfer safeguard applicable to personal data processing operations provided by a sub-processor of the service provider is identified in the relevant service description;
2. if and to the extend the parties enter into a service description and the personal data controller for the personal data that is processed may include X Group customers, the following applies:
    a. in case the service provider is located outside the EEA or a country with an Adequacy Decision, the parties hereby enter into the standard contractual clauses, module 3, which are incorporated to the Intercompany Agreement by reference.

---

[52] The Intercompany Agreement defines Adequacy Decision as, "a decision by the European Commission that a country ensures an adequate level of protection with respect to personal data."

[53] The Intercompany Agreement defines Adequacy Decision as, "General Data Protection Regulation (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)" (the General Data Protection Regulation henceforth shall be referred to as the "**GDPR**").

b. In case the service provided is located within the EEA or a country with an Adequacy Decision, the service provider shall enter into the standard contractual clauses, module 3, with its further sub processors which are located outside the EEA or country with an Adequacy Decision.

The Intercompany Agreement does not explicitly set out which law governs this Intercompany Agreement. However, it can be inferred from Article 15.1 (*Miscellaneous*), which stipulates that in case of conflict between a provision in the main part of the Intercompany Agreement and a provision in any of the Country-specific Annexes[54], the provision in the relevant Annex shall prevail. Furthermore, in the event of any conflict between the Intermediary Agreement and any European Union (henceforth, "**EU**") standard contractual clauses agreed according to Article 4 (*Restricted Transfers*), the EU standard contractual clauses shall prevail. EU standard contractual clauses are clauses that has been approved by the European Commission which ensure appropriate data protection safeguards which can be used as a ground for data transfers from the EU to third countries. Therefore, it can be inferred that two law may govern this Intercompany Agreement, which are: (i) the law of the country which requires additional regulation in the Intercompany Agreement, as indicated on the Country-specific Annex; and (ii) the law of the EU.

In this Intercompany Agreement, there is no specific clause that determines what forum is competent in the event of a dispute regarding the contents of the Intercompany Agreement. This is because the Intercompany Agreement only binds companies that are members of X group company, so that if a dispute occurs, it will be resolved through mutual discussion. However, in the event of a dispute regarding the Intercompany Agreement between PT X Indonesia and a foreign X Group Company that involves Indonesian citizens' personal data that is filed to a district court in Indonesia, such district court have the jurisdiction

[54] The Intercompany Agreement defines Country-specific Annex as "annex to the Intercompany Agreement containing additional regulations reflecting the mandatory requirements of applicable law in the respective country." The Intercompany Agreement also sets out that such additional regulation may also apply to service provider and service recipient which are not established in the relevant country.

to examine the case under Article 118 of the HIR and Article of the 100 RV. Furthermore, the court may then decide to apply Indonesian law under the center of gravity theory, seeing that the protection of Indonesian citizens' personal data is of utmost importance in the case.

B. CROSS-BORDER ACQUISITION TRANSACTIONS

Due to the globalized nature of the world, cross-border acquisition is now a common occurrence in various countries, including Indonesia. In a cross-border acquisition transaction, the ownership of a domestic company is acquired by a foreign entity, either directly or indirectly through other domestic company owned by the foreign entity. In such transaction, due diligence is usually carried out to ensure that the target company is in good condition, identify any possible issue that may hamper the transaction, or determine the reasonable price to purchase the target company. In the course of due diligence, personal data may have to be disclosed by the target company to the prospective purchaser, such as identity number of the members of the board of directors and board of commissioners.

If the above transaction occurs in Indonesia, it is important to determine the role of each parties involved to see their responsibilities under Indonesian law. The Indonesian target company (henceforth, "**Target**") and the prospective purchaser (henceforth, "**Purchaser**") can be considered as personal data controllers, being the parties that determine the purpose of personal data collection. Under the Indonesian law, it is therefore the Target's obligation to ensure that there is ensure an adequate and binding personal data protection for the data subject's personal data. The Target can also ensure that personal data subject consents to the processing of their personal data, including the transfer of their personal data abroad to the prospective purchaser. It is also important to determine the applicable law and competent forum in the event of dispute regarding the consent given by the personal data subject.

If a personal data protection dispute occurs in relation to the data subject's personal data, whether between the Target and the Purchaser or between the personal data subject and the Purchaser, Indonesian courts have jurisdiction to examine the case under Article 118 of the

HIR and Article 100 of the RV. Furthermore, seeing that the case is about the protection of Indonesian citizens' personal data the court may then decide to apply Indonesian law under the center of gravity theory.

V. CONCLUSIONS

From the research that the author has done, the following conclusions can be drawn:

1. In Indonesia, regulations regarding personal data protection is spread out among various laws and regulations, with the most recent one being the PDP Law. The PDP Law stipulates the rights of personal data subject, as well as the obligations of personal data controllers and personal data processors. The PDP Law also regulates personal data transfer carried out by personal data controllers from within the jurisdiction of Indonesia to outside the jurisdiction of Indonesia, which may only be carried out: (i) to a country that has an equivalent or higher level of personal data protection than what is stipulated in the PDP Law; (ii) by ensuring that there is an adequate and binding personal data protection; or by consent of the personal data subject. Furthermore, under Indonesian law,
2. To determine which law apply in a personal data protection dispute with a foreign element, several approaches may be used to determine the SCP, such as nationality, domicile, residence, legal seat, the place where tort occurs, the place where legal proceedings is initiated, choice of law, the place where legal action is carried out, the place where the agreement is made, or the center of gravity. To determine the competent forum in personal data protection disputes with foreign elements, there are several approaches used, in the form of the *actor sequitur forum rei* approach, the forum where the causative event occurred, the forum where the contract was executed, the mosaic approach, and the center of interest approach. Under Indonesian Law, Indonesian courts have the competency to examine cases of personal data protection with a foreign element under Article 118 of the HIR and Article 100 of the RV.

To further improve personal data protection, especially protection of personal data with a foreign element, the author would like to put forward the following suggestions:

1. for personal data controllers and personal data processors:
    a. obtaining valid and explicit consent from the personal data subject for each processing activity is of utmost importance. In the initial collection of personal data from the personal data subject, it may be efficient to request consent from the personal data subject for future activities envisaged by the personal data controller, such as personal data transfer to a third party for the purpose of due diligence. Explicit choice of law and choice of forum should also be made in any personal data processing agreement, to avoid the issue of multiple law being potentially applicable.
    b. understanding that as of now, the Indonesian PDP Institution which is authorized to carry out assessment towards the fulfilment of requirements for Personal Data transfer to outside the jurisdiction of Indonesia, which may include stipulating adequacy decision stating that a country has an equivalent or higher level of personal data protection than what is stipulated in the PDP Law has not been established, it is best for personal data controller who intends to carry out personal data transfer to outside the jurisdiction of Indonesia to ensure that there is an adequate and binding personal data protection or to obtain consent from the personal data subject.
2. for the government, including judicial institutions:
    a. increasing public awareness of the importance of protecting their personal data needs to be improved through socialization by the Ministry of Communication and Informatics.
    b. Indonesian judicial institutions need to be aware and prepared to adjudicate personal data protection with foreign elements cases. In personal data protection with a foreign element case involving Indonesian data subject's personal data that does not have a choice of law, the court may use the center of gravity

approach to ensure protection of the Indonesian data subject's rights regarding its personal data.

c. at the international level, cooperation in the formulation of regional or international conventions related to the protection of personal data needs to be carried out, in order to encourage uniform regulations regarding the protection of personal data in each country.

BIBLIOGRAPHY

Legal Documents

Council of Europe. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Council of Europe Treaty Series No. 108 (1981).

Dutch East Indies (now Indonesia). *Algemene Bepalingen van Wetgeving voor Indonesie*. (*General Provisions of Legislation for Indonesia*).

Dutch East Indies (now Indonesia). *Burgerlijk Wetboek* (*Civil Code*). Translated by Prof. R. Subekti, S.H. and R. Tjitrosudibio. Jakarta: 2017, Balai Pustaka.

Dutch East Indies (now Indonesia). *Het Herziene Indonesich Reglement*. (*Updated Indonesian Reglement*).

Dutch East Indies (now Indonesia). *Indische Staatsregeling*. (*Indian Constitution*).

Dutch East Indies (now Indonesia). *Reglement op de Burgerlijke Rechtsvordering*. (*Regulations on Civil Procedure*).

European Union. Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. OJ L 281, 23.11.1995, p. 31–50.

European Union. Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88.

Organisation for Economic Cooperation and Development (OECD). Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data.

Indonesia. *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik*. Permenkominfo No. 20 Tahun 2016 (*Minister of Communication and Informatics Regulation on the Personal Data Protection in Electronic Systems*. (MoCI Reg. 20 of 2016).

Indonesia. *Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. PP No. 71 Tahun 2019. (*Government Regulation on the Implementation of Electronic Systems and Transaction*. GR No. 71 of 2019).

Indonesia. *Undang-Undang Dasar 1945*. (*The 1945 Constitution of the Republic of Indonesia*).

Indonesia. *Undang-Undang tentang Pengesahan* International Covenant on Civil and Political Rights *(Kovenan Internasional tentang Hak-Hak Sipil dan Politik*). UU No. 12 Tahun 2005. (*Law on the Ratification of the International Covenant on Civil and Political Rights*. Law No. 12 of 2005).

Indonesia. *Undang-Undang tentang Perlindungan Data Pribadi*. UU No. 27 Tahun 2022. (*Law on Personal Data Protection*. Law No. 27 of 2022).

Indonesia. *Undang-Undang tentang Perseroan Terbatas*. UU No. 40 Tahun 2007. (*Law on Limited Liability Company*. Law No. 40 of 2007).

Indonesia. *Undang-Undang tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. (*Law on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions*. Law No. 19 of 2016).

International Covenant on Civil and Political Rights. 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976).

Universal Declaration of Human Rights. 217 A (III).

Books

Amiruddin, Zainal Asikin. *Pengantar Metode Penelitian Hukum [Introduction to Legal Research Methods]*. Raja Grafindo Persada, 2012.

Basuki, Zulfa Joko. *et al*. *Hukum Perdata Internasional [Private International Law]*. Universitas Terbuka, 2014.

Gautama, Sudargo. *Hukum Perdata Internasional Indonesia Jilid III Bagian I Buku ke-7 [Indonesian Private International Law Volume III Part I 7th Book]*. PT Alumni, 2010.

Gautama, Sudargo. *Pengantar Hukum Perdata Internasional Indonesia [Introduction to Indonesian Private International Law]*. Binacipta, 1987.

Holvast, J. "The Protection of Privacy." in *The History of Information Security: A Comprehensive Handbook*, edited by Karl de Leeuw and Jan Bergstra. Elsevier Science, 2007.

Marton, Edina. *Violations of Personality Rights through the Internet: Jurisdictional Issues under European Law*. Nomos, 2016.

Soekanto, Soerjono. *Pengantar Penelitian Hukum [Introduction to Legal Research]*. UI Press, 2015.

Voigt, Paul and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR*). Springer Nature, 2017.

Journal

Bigos, Oren. "Jurisdiction over Cross-Border Wrongs on the Internet." *The International and Comparative Law Quarterly* 54 (2005): 585-620.

Lutzi, Tobias. "Internet Cases in EU Private International Law-Developing A Coherent Approach." *International and Comparative Law Quarterly* 66 (2017): 687-721.

Mangku, Dewa Gede Sudika. *et al*. "The Personal Data Protection of Internet Users in Indonesia." *Journal of Southwest Jiaotong University* 56 (2021): 202-209.

Mantelero, Allesandro. "The Future of Data Protection: Gold Standard vs. Global Standard." *Computer Law & Security Review* 40 (2021): 1-7.

McManus, Hugh S. "Conflict of Laws: The "Center of Gravity" Theory Applied to Torts: Babcock v. Jackson". *Marquette Law Review* 47 (1963): 255-264.

Internet

Clement, J. "Market Value of the Largest Internet Companies Worldwide 2021." https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/. Accessed 18 April 2022.

Data Reportal. "Digital 2021: Indonesia." https://datareportal.com/reports/digital-2021-indonesia. Accessed 7 February 2022.

Data Reportal. "Digital 2022: Global Overview Report." https://datareportal.com/reports/digital-2022-global-overview-report. Accessed 7 February 2022.

European Union. "Types of Legislation." https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en. Accessed 18 April 2022.

Semrush. "Most Visited Websites by Traffic in Indonesia for all categories, June 2022." https://www.semrush.com/website/top/indonesia/all/. Accessed 8 February 2022.

Others

X Group Company. Intercompany Agreement on Data Processing. 27 September 2021.

Tisnadisastra, Abadi Abi. "Introduction to Indonesia Personal Data Protection Regulatory Framework." The presentation was delivered at the Days of Law Career 2022 workshop, Depok, 11 February 2022.