PERSONAL DATA: COMPARATIVE STUDY BETWEEN INDONESIAN MINISTERIAL REGULATION AND EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

Muhammad Dwistaraifa Rasendriya[1]

Abstract

The ubiquity of personal data online triggers the need to regulate the processing, storage and the deletion of such data. Within the territory of the European Union, its transfer (even past its boundaries) and processing of personal data are subject to the General Data Protection Regulation (GDPR) and its jurisprudence. Article 45(1) of the GDPR empowers the European Commission to issue an Adequacy Decision, which compares the regime of a third country against the GDPR and its jurisprudence. Its issuance would allow seamless transfer of personal data to third country. This provision begs the question if Indonesian legal landscape on data protection meets the yardsticks contained in GDPR.

This editorial will introduce the regimes in European Union and Indonesia, analyse the pertinent Indonesian legislation on the subject, in light of the GDPR, along with the jurisprudence of the Court of Justice of the European Union on the matter. This paper concludes that the Indonesian present data protection regime is extremely lacking, notably due to its narrow scope of application, weak watchdog authority, and its feeble punishment for its violation.

Intisari

Merebaknya penyebaran data pribadi di dunia daring melahirkan kebutuhan untuk meregulasi penggunaan, penyimpanan dan penghapusan data ini. Di dalam kawasan Uni Eropa, transfer (bahkan melewati batas-batasnya) dan pengolahan data pribadi diatur oleh Regulasi Umum Perlindungan Data Pribadi (GDPR). Pasal 45(1) dari GDPR memberikan kuasa kepada Komisi Uni Eropa untuk menerbitkan Keputusan Kecukupan, yang berisikan perbandingan kerangka kerja perlindungan data pribadi di negara ketiga terhadap GDPR dan yurisprudensinya. Penerbitan Keputusan ini akan mengizinkan perpindahan data pribadi tanpa batas ke negara ketiga itu. Pasal ini menimbulkan pertanyaan, sekiranya iklim hukum Indonesia di ranah perlindungan data pribadi memenuhi persyaratan yang terkandung dalam GDPR.

Editorial ini akan memperkenalkan rezim-rezim Uni Eropa dan Indonesia, menganalisa hukum Indonesia di ranah ini dengan sudut pandang GDPR, bersamaan dengan yurisprudensi Mahkamah Keadilan Uni Eropa di topik ini. Artikel ini menemukan berbagai kelemahan di rezim perlindungan data pribadi Indonesia, dikarenakan sempitnya ranah aplikasi, lemahnya kekuatan badan pengawas dan lemahnya hukuman atas pelanggarannya.

Keywords: data protection, Indonesia, GDPR, European Union, Ministry of Communication and Informatics

Kata Kunci: perlindungan data, Indonesia, GDPR, Uni Eropa, Kementerian Komunikasi dan Informatika

[*] Muhammad Dwistaraifa Rasendriya, LL.B. candidate of Maastricht University, Class of 2017; S.H. Candidate of Universitas Gadjah Mada, Class of 2016

A. Introduction

The Internet has transformed much of the society for the past 20 years. It brings access to once-secluded knowledge, it connects one person to another in different continents instantaneously. Recital 6 of the General Data Protection Regulation ("**GDPR**") of the European Union ("**EU**") sums the situation best:[1] "Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally." However, it must be noted that it is not as easy for these natural persons to take down their personal information offline. As a popular saying goes, "internet does not forget."

This pervasiveness of personal data put online also possesses enormous economic value, as found by the European Union Agency for Cyber Security in 2017.[2] It would facilitate a targeted advertisement to 3.8 billion internet users, who would raise around US$59/user in revenue that year. This targeted advertisement was also the crux of the Cambridge Analytica scandal, which saw the personal data of 87 million Facebook users harvested by a political consulting firm,[3] and utilised to the benefit of an American presidential candidate. Next to the economic value that personal data possesses, the example of Cambridge Analytica shows the potential political impact which collection of personal data has.

Next to the aforementioned points, the connectivity of the internet exposes a risk where a personal data could be transferred to a country whose data protection law is much weaker or non-existent in order to circumvent the application of a stringent data protection legal regime. This surely defeats the purpose of legislating on the processing and disposal of personal data within the boundary of one country. These three factors show the need for the government to regulate the collection, processing, disposal and transfer of personal data beyond its own boundary.

This article will introduce each legal regime briefly, and compare among themselves provisions regarding the scopes of application, collection, processing, and transfer of personal data to a third country. It will conclude with pointers and suggestions on where can Indonesia improve its data protection regime.

a. *The European Union's GDPR*

The GDPR[4] is the result of the European Commission's Proposal 2012/0011.[5] It was intended to overcome the shortcomings of the previous legislation, Directive 95/46/EC (Directive

---

1 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) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 2. (Accessed: https://eur-lex.europa.eu/eli/reg/2016/679/oj on 01/01/2020).

2 The Value of Personal Online Data. (2018, April 23). Accessed: https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data on 01/01/2020).

3 Kang, C., & Frenkel, S. (2018, April 4). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. Retrieved January 1, 2020, from https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html?action=Click&contentCollection=BreakingNews&contentID=66776835&pgtype=Homepage.

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L

95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data).[6] Based on Article 16 of the Treaty on the Functioning of the European Union, everyone within the territory of the European Union has the right to have their personal data protected.[7] The GDPR introduces the general rule that processing personal data is illegal, unless the data subjects consent to the processing (Article paragraph 6(1)). Article 7 of the GDPR describes the standard of a lawful expression of consent. The GDPR also enumerates data subjects with a variety of rights which they can directly exercise *vis-à-vis* the data processors and controllers. For these reasons, many have applauded the GPDR to be the gold-standard of data protection legislation.[8]

A national Data Protection Authority ("**DPA**"), who may also be the lead authority within the territory of a member state, enforces the GDPR (Article 51). The authority also works on European-level as a part of the European Data Protection Board (Article 68), whose task is ensuring the uniform enforcement of the GDPR throughout the EU (Article 70). The GDPR grants these national DPAs power to impose steep fine for its infringement. Depending on the violations, it may either impose a fine as high as 10 million Euros or 2% of the amount of annual turnover (Article 83(4)), or a fine capped at 20 million Euros or 4% of the annual global turnover (Article 83(5)).

It must be noted that a European Union Regulation is distinct from a European Union Directive. A Regulation is directly enforceable the moment it comes into force;[9] unlike a Directive which contains mere goal for the policy and must first be transposed into the domestic legislation of respective member states.[10]

Therefore, the GDPR is directly enforceable as a source of law before the courts of member states of the EU; this is different from a Directive which must first be transposed. However, it leaves some room for discretion for respective member states to introduce deviations. This article will only keep to GDPR itself, and not its disparate domestic implementation acts in the member states of the EU.

119, 4.5.2016, p. OJ L 119, 4.5.2016, p. 1–88. Accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1578453414390&uri=CELEX:32016R0679; accessed on 17/12/2019.

5 Proposal for a Regulation of Proposal for a Regulation 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 (General Data Protection Regulation), COM (2012) 11 - C7-0025/12; accessible via http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf; accessed on 01/01/2020.

6 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

7 Treaty on the Functioning of European Union, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT; accessed on 31/12/2019.

8 Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall L. Review, 47, 809, p.813.

9 Judgment of the Court of 17 September 2002, *Antonio Muñoz y Cia SA and Superior Fruiticola SA v Frumar Ltd and Redbridge Produce Marketing Ltd*, Reference for a preliminary ruling: Court of Appeal (England & Wales) (Civil Division) - United Kingdom, ECLI:EU:C:2002:497, par. 27; Article 288 of Treaty on the Functioning of European Union, accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT; accessed on 31/12/2019.

10 Judgment of the Court of 4 December 1974, *Yvonne van Duyn v Home Office*, Reference for a preliminary ruling: High Court of Justice, Chancery Division - United Kingdom, Case 41-74, ECLI:EU:C:1974:133, par 12; Judgment of the Court of 5 April 1979, Reference for a preliminary ruling: Pretura di Milano – Italy, Case 148/78, ECLI:EU:C:1979:110, par 24.

b. ***Indonesian Legal Landscape***

Indonesia has yet to legislate an all-encompassing general statute on data protection at the same extent as the GDPR. However, this does not mean that the concept of personal data protection is a foreign one. Article 28G of Amended Indonesian 1945 Constitution provides that everyone is entitled to protection *inter alia* their dignity and property.[11] It must be noted that there are various provisions for data protection in different legislations and regulations. Most of these legislations and regulations deal with very specific subject-matter. Presently, the following regulations and legislations mentioned the need for data protection in passing, without much elaboration:[12]

1) Law No. 7/1992 regarding Banking as amended by Law No. 10/1998 (the Banking Law);
2) Law No. 39/1999 regarding Human Rights;
3) Law No. 23/2006 regarding Resident Administration as amended by Law No. 24/2013 (the Resident Law);
4) Law No. 36/1999 regarding Telecommunications (Telecommunications Law);
5) Law No. 14/2008 regarding Transparency of Public Information;
6) Law No. 36/2009 regarding Health (the Health Law);
7) Law No 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No 19 of 2016 (Electronic Transactions & Information Law; the "ETI" law)
8) Minister of Health Regulation No. 269/Menkes/Per/III.2008 on Medical Records (MoH Regulation 269);
9) Minister of Communication and Informatics ("MoCI") Regulation 36/2014 on the Registration Procedure of Electronic System Operator;
10) MoCI Regulation 20/2016 on Protection of Personal Data of MoCI;
11) MoCI Regulation 04/2016 on the Information Security Management System (MoCI Regulation 4);
12) Financial Services Authority (Otoritas Jasa Keuangan or "OJK") Regulation No. 1/POJK.07/2013 regarding financial consumer protection;
13) Government Regulation 82/2012 on Provision of Electronic System and Transaction

From this list, MoCI Regulation 20/2016 on Protection of Personal Data of the Ministry of Communications and Informatics ("The Regulation") is of interest. Article 26 of the ETI Law merely defines what is considered "privacy", and establishes that any usage of a personal data must be done with consent.[13] The Government Regulation 82/2012,[14] being the

---

[11] Amended Indonesian Constitution. (n.d.). Retrieved January 1, 2020, from http://www.dpr.go.id/jdih/uu1945. Unofficial English translation accessible via: http://www.unesco.org/education/edurights/media/docs/b1ba8608010ce0c48966911957392ea8cda405d8.pdf.

[12] Tisnadisastra, A. A., Prasetyo, P. S., & Adwani, F. (2019). *Indonesia*. Data Protection & Privacy 2020. (A. P. Simpson & L. J. Sotto, Eds.). London: Law Business Research Ltd, p.119.

[13] Law No 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No 19 of 2016, accessible via: http://www.gmf-aeroasia.co.id/wp-content/uploads/bsk-pdf-manager/11_UU_NO_11_TAHUN_2008_TENTANG_INFORMASI_DAN_TRANSAKSI_ELEKTRONIK.PDF and https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf ; accessed on 31/12/2019.

[14] Indonesian State Journal no. 189, 2012; accessible via: (http://ditjenpp.kemenkumham.go.id/arsip/ln/2012/pp82-2012bt.pdf

implementation act of the Law, defines what is personal data and imposed obligations on the service provider *vis-a-vis* the owner of the personal data.

The Ministerial Regulation is the relevant Indonesian regulation in force at the moment given its specificity and prevalence of electronic storing and processing of personal data, given that the general Data Protection Bill was only transmitted to the Indonesian Parliament in December 2019.[15] As the implementing act for Law 11/2008 on Electronic Transaction, and Government Regulation 82/2012 on Provision of Electronic System and Transaction, its main purpose is to establish the details for protection of personal data within electronic environment.

The MoCI Regulation does so by identifying the personal scope, material scope, as well as principles and general rules of digital storage and processing of personal data. Next to this, it also sets up a dispute resolution process for infringement of the Regulation or data leaks. The following sections will elaborate on these points. Application.

c. *Material & Territorial Scope of the GDPR*

Territorial application of the GDPR is contained in Article 3: it applies where the processor or controller is established in the territory of EU, or if they offer goods and services to data subjects in the EU; regardless if payment is required. In *Google Spain*,[16] it was found that a mere business activity in an EU member state suffices for the GDPR to apply; no need for a fully-established subsidiary.

Materially, the GDPR applies whenever a processing of personal data is involved (Article 2). It contains a broad definition of personal data; if it can directly, or indirectly, identify a person, be it an ID number, or any reference to their specific factors, it will be considered as a personal data. Next to defining what is personal data, the GDPR also prohibits processing special category of personal data.[17] This is the data which may reveal sensitive data such as political leaning, trade union membership or one's sexual orientation or sex life. Exception to this general prohibition exists in an exhaustive list in Article 9 paragraph (2).

It defines "processing" broadly; it is whenever an operation, or set of operations, is done on the personal data, or a set of it; automated or manually done (Article 4(2)). The Article mentions examples of processing, such as: collection, recording, organisation of such data, storage, or even destruction. The legislator intended such expansive definition to preclude any attempt to evade its application, and to preempt any technological advances (cf. Recital 15). Regarding manual processing, the GDPR applies when the following criteria are fulfilled:[18] the data must be placed in a filing system, and that it is sorted according to a specific criterion.

---

[15] Information and Telecommunications Minister: Draft Data Protection Bill soon handed to Parliament(Rahma, A. (2019, December 19). Menkominfo: Draf RUU Perlindungan Data Pribadi Segera ke DPR. Retrieved January 1, 2020, from https://nasional.tempo.co/read/1285533/menkominfo-draf-ruu-perlindungan-data-pribadi-segera-ke-dpr/full&view=ok);.

[16] Judgment of the Court (Grand Chamber), 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317, par 55.

[17] Article 9(1) of the General Data Protection Regulation, n.4.

[18] Judgment of the Court (Grand Chamber) of 10 July 2018, Proceedings brought by Tietosuojavaltuutettu, C-25/17, ECLI:EU:C:2018:551, paras. 56 & 58.

Based on this definition, processing could be as simple as taking down personal contact information by hand and classify it into different sections,[19] pointing CCTV in direction of a public space,[20] or even displaying one's data on the internet.[21]

The GDPR contains list of exceptions from its application, as contained in Art 2(2). The relevant exception for most people is processing that is purely for personal or household use.[22] The Court of Justice of the European Union in *Ryneš v Úřad pro ochranu osobních údajů*[23] has found that if a processing intrudes into, or visible from, public space, then it is not personal use. It also does not apply to anonymised data,[24] *i.e.* data which does not identify a specific natural person.[25] Processing of pseudonymised *i.e.* data which may not identify without the use of additional information,[26] is allowed; provided that the personal data and the identifying information are kept separately, and that the identifying information are subject to organisational and technical measures.[27] It is a way to for the controllers and processors to meet their data protection obligation,[28] not a mean to preclude its application.

d. ***Material & Territorial Scope of Indonesian MoCI Regulation***

MoCI Regulation applies to collection, processing, storage, display, dissemination as well as destruction of personal data within an electronic environment (Article 3). There is no further elaboration on this point. It makes no mention of its territorial scope, although its parent legislation, the ETI Law has extraterritorial application.[29] Thus it has been argued that the Regulation, being derived from ETI Law, also possesses extraterritorial character.[30]

It defines Personal Data ("*Data Pribadi*") being a data which are kept, maintained, kept up to date and kept secret (Article 1). It also defines Certain Personal Data ("*Data Perseorangan Tertentu*"): data which are real, and true, which relates to a person and may identify them indirectly or directly (Article 1 paragraph (2)). This definition, does not diverge from GDPR's definition; the two definitions pertain to a data which may directly, or indirectly, single out a person. However, it lacks the definition of special personal data in sense of Article 9 of the GDPR. Indonesia should consider defining and regulating such type of data in its future data protection legislation, given its diversity of peoples.

Regarding the material scope of MoCI Regulation, it is pretty much similar to the GDPR and its jurisprudence, one clear weakness is that it does not apply to manually-collected and -kept

---

19 *Supra*, para 36.

20 Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš v Úřad pro ochranu osobních údajů*, Case C-212/13, ECLI:EU:C:2014:2428, par 33.

21 Judgment of the Court of 6 November 2003, Criminal proceedings against Bodil Lindqvist, Case C-101/01, ECLI:EU:C:2003:596, par 23.

22 Article 2 paragraph (2) letter (c) of the General Data Protection Regulation, n.4.

23 Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš v Úřad pro ochranu osobních údajů*, Case C-212/13, ECLI:EU:C:2014:2428, par 33.

24 Article 3 & 4 paragraph (1) of the General Data Protection Regulation, n.4.

25 Voigt page 13;

26 Article 4 paragraph (5) of the General Data Protection Regulation, n.4

27 *Ibid*.

28 Recital 28 of the General Data Protection Regulation, n.4

29 Article 2 of Law No 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No 19 of 2016, n.13.

30 Zacky Zainal Husein & Muhammad Iqsan Sirie (Assegaf Hamzah & Partners), Indonesia: Data Protection 2019, accessible via: https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia; accessed on 02/01/2020.

personal data. One may argue that it is the product of the Ministry of Communication and Informatics, who is the authority in things digital and electronic in the country. However, this weakness makes the MoCI Regulation considered not equally-effective to the GDPR since it will not provide a complete protection which the GDPR and European Law sought to provide to personal data:[31] the MoCI Regulation would be easily circumventable by writing the information down manually and kept in a written form.

e. ***Personal Scope of the GDPR***

It applies to anyone processing or controlling personal data. A processor is a party which processes the data on its own behalf, or the controller's (Art 4 paragraph (7)). Meanwhile, the controller is the party which determines the purpose of processing (Art 4 paragraph (8)). A controller may be a natural or legal person, alone or jointly determines the purpose of processing. A processor must be a separate party from the controller, and processes the personal data on the *behalf* of the controller. Such cooperation must be put in a contract.[32] This contract should be specific to each relationship to best protect the parties involved.[33] In the jurisprudence of the Court of Justice of the European Union, both the controller and processor are responsible to protect the personal data of the Data Subjects.[34]

f. ***Personal Scope of Indonesian MoCI Regulation***

The MoCI does not explicitly mention it. However, the Regulation names User ("*Pengguna*"),[35] Provider of Service ("*Penyelenggara Sistem Elektronik*"), and Owner of Personal Data ("*Pemilik Data Pribadi*"). These terms are comparable to "Processor", "Controller", and "Data Subjects" in the terms of the GDPR, based on the respective role and responsibility of each actors. In the MoCI Regulation, only the User (i.e. Processor) who is responsible to protect the personal data (Article 27). This point diverges heavily with that of the GDPR's jurisprudence, where both controller and processor bear the responsibility to protect the data; not only the latter. Asdqwe

B. <u>Collection of Personal Data</u>

a. ***GDPR's Collection***

Article 5 of the GDPR contains the six principles which must be followed in collecting (*i*.e. processing) the personal data. These principles are: lawfulness, fairness, and transparency,[36]

---

[31] Lindroos-Hovinheimo, S. (2018). Who controls our data? The legal reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v Jehovan todistajat. Information & Communications Technology Law, 28(2), 225–238, p.230.

[32] Article 28 paragraph (3) of the GDPR, n.4.

[33] Fielding, R. (2018). The Concept of Controller and Processor Data Entities. Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns, 2, 1–13. p.9.

[34] Judgment of the Court (Grand Chamber) of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Case C-210/16, ECLI:EU:C:2018:388, paras. 32 & 35.

[35] Article 1 paragraph (7) of MoCI Regulation 20/2016 ("The MoCI Regulation"), Indonesian State Journal no 1829/2016. Accessible via https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016; accessed 10/11/2019.

[36] Article 5 paragraph (1) letter (a) of the GDPR, n.4

purpose limitation[37], data minimisation[38], accuracy[39], storage limitation[40], integrity and confidentiality.[41]

1. Principles

i. Lawfulness, fairness and transparency

These principles combined make up one principle. Lawfulness & fairness principles demand that a legal permission allows the processing done fairly, or that it was consented by the data subject.[42] Transparency principle demands that the data subject knows who the controller is, the purpose of the processing, their right to confirmation and communication on the processing done to their data. Next to this, the data subject should also be notified of the risk, rule, safeguard and their right regarding to the processing. Any information on the last point must be in accessible, easily comprehensible, in clear and plain language.[43]

These principles are reflected in Articles 13 and 14 of the GDPR regarding the obligation of the controller to inform the data subjects when their data is being collected. The controllers must provide information listed in the articles, depending on the circumstance of the collection, collected directly from the data subjects (Article 13) or indirectly (Article 14). The Recitals 60-62 of the GDPR help elaborating what information must be present as well as an option how to fulfill it.

ii. Purpose limitation

Data should only be processed for a specific, explicit, and legitimate purpose.[44] No further processing which goes against that purpose is allowed. This is important to determine the lawfulness of the processor's or controller's activities.

iii. Data minimisation

Only relevant and adequate personal data which are limited to the purpose of the processing is used during processing.[45] The parties themselves should enquire what data is required for the processing.[46] This is an obligation of minimal data collection *vis-a-vis* the processing purpose, *i.e.* the collected data must be adequate for the processing purpose, and not further.[47]

iv. Accuracy

---

[37] Article 5 paragraph (1) letter (b) of the GDPR, n.4
[38] Article 5 paragraph (1) letter (c) of the GDPR, n.4
[39] Article 5 paragraph (1) letter (d) of the GDPR, n.4
[40] Article 5 paragraph (1) letter (e) of the GDPR, n.4
[41] Article 5 paragraph (1) letter (f) of the GDPR, n.4
[42] Recital 39 of the GDPR, n.4.
[43] Recital 58 of the GDPR, n.4.
[44] Recital 23 of the GDPR, n.4.
[45] Recital 39 of the GDPR, n.4
[46] VOIGT, PAUL. VON DEM BUSSCHE, AXEL. (2018). Eu General Data Protection Regulation (Gdpr): a practical guide. S.l.: SPRINGER INTERNATIONAL PU. P.90.
[47] *Ibid.*

Every reasonable step must be taken to ensure that data that is inaccurate, having regard to the purposes of the processing, is erased or rectified without delay.[48] This principle is reinforced by the right to rectification and erasure of the personal data of the data subjects, contained in Articles 16 and 17 paragraph (1) of the GDPR. The Right to be Forgotten is now contained in Article 17 paragraph (2) of the GDPR, it has been recognised as a fundamental right under Articles 7 and 8 of Charter of Human Rights of the European Union.[49]

v. Storage limitation

Personal data should be kept in such form and manner that which allow identification of data subjects for as long as it is necessary for the processing.[50] The storage period shall be limited to a strict minimum,[51] i.e. only as long as it is necessary for processing.

vi. Integrity and Confidentiality

The personal data must be processed in a manner which assures its security from risks such as unauthorised or unlawful processing and against accidental loss, destruction or damage, by deploying appropriate technical and organisational measures. The GDPR elaborated at length on the organisational measures in its provisions.

b. *The MoCI Regulation Collection - principles*

The Second Section of the MoCI Regulation elaborates on the principles applicable to the collection and gathering of personal data. These principles are data minimisation, relevance, accuracy[52] private[53] and consensual & legitimate.[54]

It is lamented that the MoCI Regulation does not elaborate these principles at length, to the extent of the GDPR does. This circumstance makes these principles unsuitable to enforce since it is unclear what the yardstick for compliance is. The Data Protection Bill should cover this loophole by elaborating on what these principles actually mean.

Regarding the different collection circumstances, the MoCI Regulation merely demands that if the data was collected directly from the Owner of Personal Data, it must be immediately verified;[55] if it was collected indirectly, it must be verified based on different data sources.[56]

C. <u>Processing of Personal Data</u>

a. *The GDPR's processing*

As elaborated *supra* in section B.a., the GDPR adopts a broad definition to the term "processing". The legislator intended the definition to preempt future technological developments, thus ensuring its far-reaching application. Article 5 of the GDPR contains the

---

48 Article 5(1)(d) of the GDPR, n.4.
49 Judgment of the Court (Grand Chamber), 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317, par 97.
50 Article 5 paragraph (1) letter (e) of the GDPR, n.4.
51 Recital 39 of the GDPR, n.4.
52 Article 7 paragraph (1) of the MoCI Regulation
53 Article 8 paragraph (1) of The MoCI Regulation
54 Article 9 paragraph (1) of The MoCI Regulation
55 Article 10 paragraph (1) of MoCI Regulation
56 Article 10 paragraph (2) of MoCI Regulation

principles which must be followed in processing of personal data. Having elaborated that, it must be borne in mind that the GDPR introduces the general prohibition on processing, unless it was consented by the data subject. In this regard, the GDPR provides an exhaustive list for conditions to legitimate consent. It is contained in Article 7. The *onus* that the data subject consented lies with the controller.[57]

Regarding consent, it must be mentioned that there is a specific provision for consent provided by minors under 16 years old in the GDPR. This provision stipulates that the minor's guardian or parental consent take the place that of the minor's until they attain the age of 16.[58] In this regard, the MoCI Regulation does not differ much from the GDPR, aside from the fact that it does not lay a specific age for one to be considered "minor" but rather conceding that to other statutory limit.[59]

b. ***The MoCI Regulation's processing***

The Section Three of the MoCI Regulation provides for processing ("Processing and Analysis of Personal Data"), processing of personal data according to MoCI Regulation follows different principles from those which apply during collection. Succeeding section deals with storage ("Storage of Personal Data"). The following principles are those which apply during processing:

Purpose limitation[60] Consensual[61] Accurate[62]

Aside from explaining that purpose limitation principle is an obligation, where the Provider of Service (*i.e.* Controller) is to determine the extent and purpose of the collected data, the MoCI Regulation does not elaborate how or what these principles apply in practice.

An exception to consensual principle is contained in Article 13 of the MoCI Regulation: it states that data shown publicly *on* the Electronic System or declared as public *by* the Electronic System (i.e. any electronic device which does the processing, storage, displaying etc).[63] This could be an attempt to emulate an exception in the GDPR regarding the Right to be Forgotten under Article 17(2), but it lacks such context. To allow this exception to stand as it is, may lead to a situation where no data could be protected, since it was displayed publicly on a website (e.g. a Facebook profile name). The upcoming bill on Data Protection should provide recitals to better interpret and elaborate this provision.

D. <u>Deletion of Personal Data</u>

a. ***The GDPR's Deletion***

Given the broad definition of "processing" which thus includes deletion of personal data, the GDPR principles on processing regulate the deletion personal data. See section C.a.i for

---

[57] Article 7 paragraph (1) of the GDPR, n.4.
[58] Article 8 paragraph (1) of the GDPR, n.4.
[59] Article 37 of the MoCI Regulation.
[60] Article 12 paragraph (1) of the MoCI Regulation
[61] Article 12 paragraph (2) of the MoCI Regulation
[62] Article 14 of the MoCI Regulation
[63] Article 1 paragraph (5) of the MoCI Regulation

elaboration on these principles. The Right to Erasure will be addressed by Section G of this article, as a part which deals on the right of data subject.

b. *The MoCI's Deletion*

Section Six of the MoCI Regulation regulates the destruction of the personal data which the Provider of Service (*i.e.* Controller) or User (*i.e.* Processor) manage. Erasure can only be done only if the Owner of Personal Data (*i.e.* Data Subject) specifically requests deletion of their personal data,[64] or if the storage has exceeded the time limit stipulated within the MoCI Regulation or any other regulations or statute[65] (the MoCI Regulation does not stipulate a time limit itself; it merely wrote in the provision on data storage, that the data must be kept for at least five years[66]). Interestingly, despite laying down that personal data protection only occurs in an electronic/digital environment, the disposal of personal data must also entail destruction of *all* documents in electronic as well as non-electronic forms.[67]

This could be an editorial oversight that the MoCI Regulation does not lay down a specific deadline. Regardless, this issue better be addressed in the upcoming Data Protection Bill in order to ensure its strong enforcement, since such deadline would give a clear yardstick.

E. A Third Country Transfer of Personal Data

a. *The GDPR's transfer*

The GDPR provides general principle of data transfer to a third country (any country outside the European Union) in Article 44. It also governs onward transfer (*i.e.* transfer from that third country to another third country).[68] The data can only be transferred provided that the controller and processor comply with the conditions contained in the provisions of the section. There are different modalities for a seamless transfer of data to happen:[69]

1. Adequacy decision

Article 45 paragraph (1) of the GDPR confers authority on the European Commission to determine and issue an Adequacy Decision, which would certify the data protection regime of a third country is adequate according to the GDPR standard. This would allow an impeded data transfer between an EU member state with that third country. Article 45 paragraph (2) describes the different aspects of the third country's data protection regime which will be assessed against the GDPR.

In order for a regime to attain an "adequate" level of protection, it must not necessarily be identical with the GDPR.[70] However, it must be equally-effective.[71] In other words, the level of

---

[64] Artcile 25 paragraph (1) letter (b) of the MoCI Regulation
[65] Article 25 paragraph (1) letter (a) of the MoCI Regulation
[66] Article 15 paragraph (b) letter (2) of the MoCI Regulation.
[67] Article 25 paragraph (2) of the MoCI Regulation
[68] Recital 110 of the GDPR, n.4.
[69] The EU Transfers of data to UK post-Brexit: The GDPR perspective. (2018). International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, , 1., pp.8-12.
[70] Recital 10, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) OJ L 207, 1.8.2016, p. 1–112, p. 2. Accessible via: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1578552837162&uri=CELEX:32016D1250; accessed on 05/01/2020.

protection must be effective, *i.e.* the data subjects must be able to rely on the mechanism to enforce their claims.[72]

Given the scope of this paper, the remaining modalities which are: 1) appropriate safeguards and 2) binding corporate rules will not be elaborated. Nonetheless, the reader must know that other bases for a third country transfer exist.

2. **Exceptions**

The GDPR contains a strict, and exhaustive list of exceptions to the general rule contained in Article 44. In Article 49 paragraph (1) of the GDPR, it provides certain circumstances where such rule is negated. Among these circumstances is an express & specific consent of the data subject, in light of all appropriate and necessary information that the data may not be enjoying the same level of protection in the third country.[73]

b. ***The MoCI Regulation's transfer***

The MoCI Regulation covers overseas transfer in Article 22. It stipulates that any overseas transfer of data must be: 1) coordinated with the Minister or relevant authority/official,[74] and it must adhere to the statute pertaining overseas transfer of personal data.[75] In coordinating with the authorities, the notification must contain the destination, the purpose of transfer, the date of transfer as well as clear identity of the recipient.[76]

The MoCI Regulation does not regulate a standard for that destination country, neither does it address the matter further. The Data Protection Bill must address this loophole, otherwise personal data of Indonesians could be sent to a country where data protection regime is non-existent.

F. <u>Rights of Data Subject</u>

a. ***Catalogue of rights***

As elaborated *supra*, the GDPR enumerates data subject with numerous rights which they may then exercise *vis-a-vis* controller and processor. In its Chapter III, the GDPR contains various rights intended for the data subjects to exercise. These rights, as contained in Articles 12-22 include the right to receive information regarding the purpose of processing, the contact information of the data protection officer of the controller and processor, to right to not be subjected to automated decision-making. This section will focus on those rights as contained in the MoCI Regulation. It must be noted, that the GDPR's catalogue of rights is much more extensive and more-elaborated than the MoCI Regulation's.

According to the MoCI Regulation, an Owner of Personal Data has right to the secrecy to their personal data,[77] to report an infringement by Provider of Service's failure to protect their

---

71 *Ibid.*
72 *Maximillian Schrems v Data Protection Commissioner*, Judgment of the Court (Grand Chamber) of 6 October 2015, C-362/14, ECLI:EU:C:2015:650, paras. 73-74.
73 Article 49 paragraph (1) letter (a) of the GDPR, n.4.
74 Article 22 paragraph (1) letter (a) of the MoCI Regulation
75 Article 22 paragraph (1) letter (b) of the MoCI Regulation
76 Article 22 paragraph (2) of the MoCI Regulation
77 Article 26 letter (a) of the MoCI Regulation

data to the Minister,[78] to access or update their data without disturbing the Electronic System, subject to prevailing law,[79] to access their historical data,[80] subject to prevailing law, and lastly demand destruction of their data which are managed by Provider of Services, subject to prevailing law.[81] But this catalogue does not make clear the recipient of the claims of the Data Subjects. The closest thing is the right to report breach to the Minister. This provision renders the Regulation to be much weaker than the GDPR, which grants Data Subjects a list of rights enforceable towards either the processor or controller.

One may argue that the obligation to maintain a compatibility and interoperability of the Electronic System contained in Article 11 could be comparable as the right to data portability contained in the GDPR's Article 20, however, considering it addresses the User (i.e. Processor) and the Provider of Services (i.e. controller), this is not comparable to GDPR's Right to Data Portability which explicitly endowed the data subject such right.

Another deviation is the GDPR does not endow this explicit right to data secrecy to data subject. Instead it was an obligation imposed on the processor and controller.[82] The remaining rights listed prior are comparable to: the right to effective judicial remedy (against the processor, controller or the supervisory authority),[83] right to access[84] & right to rectification[85] and right to erasure in Article 17 of the GDPR.

Regarding the right to erasure, this right must be proven to exist by the requesting data subject, based on the different circumstances as listed in Article 17 paragraph (1) letters (a) to (f). Next to the right to erasure, the data subject can also exercise their right to be forgotten under Article 17 paragraph (2) of the GDPR, that it has been recognised as a fundamental right under Articles 7 and 8 of Charter of Human Rights of the European Union.[86] It must be noted that this right as contained in the GDPR is much more far-reaching than the one contained in *Google Spain* judgment.

It demands the controller to notify the processor (and anyone who receives the data concerned) within reasonable steps, bearing in mind available technology and technical cost, of request of erasure from the data subject. The processor must then delete any link, any information, original or replication, of that data.

At the moment, the MoCI Regulation has no comparable right to right to be forgotten, or other rights beyond those mentioned *supra*. Future Data Protection Bill must expand these rights in order to provide a more complete protection of one's personal data.

---

78 Article 26 letter (b) of the MoCI Regulation
79 Article 26 letter (c) of the MoCI Regulation
80 Article 26 letter (d) of the MoCI Regulation
81 Article 26 letter (e) of the MoCI Regulation
82 Article 90 of the GDPR, n.4.
83 Articles 78-79 of the GDPR, n.4.
84 Article 15 paragraph (1) of the GDPR, n.4.
85 Article 16 of the GDPR, n.4.
86 Judgment of the Court (Grand Chamber), 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317, par 97.

b. ***Supervisory authority***

1. **In GDPR**

As stipulated *supra*, the GDPR is enforced on the national level by a national data protection authority (the DPA) (Article 51). Coherence of the enforcement is coordinated on European-level by European Data Protection Board (Article 68). This national DPA must maintain a total independence, with regards to its staff, finance, and exercise of its power.[87] Its list of authority is contained in Article 58 of the GDPR, and that includes the power to investigate,[88] issue warnings,[89] orders,[90] or fine (depending on the provisions of Article 83 and 84).[91] It can also act as a party to a judicial proceeding to enforce the GDPR.[92]

2. **In the MoCI Regulation**

According to the MoCI Regulation Article 35 paragraph (1), the monitoring and enforcement of the Regulation is done by the Minister of Communication and Informatics, and/or the chief of supervisory authority and sector regulator. There is no further elaboration on who could these chief or sector regulator be. On this point, the MoCI Regulation highly diverges from the GDPR. Its supervisory authority is not independent of the government. However, it must be borne in mind that the MoCI Regulation could only go so far in establishing new powers and entity. In enforcing MoCI Regulation, the Minister cannot go further than it may listing the violators on a list as a form of administrative sanction (Article 36). Other forms of sanction include verbal warning, written warning, or an order to stop its activities temporarily.[93]

With that being said, the Data Protection Bill must provide for an independent supervisory authority, and make it the lead authority in issues pertaining to data protection. Next to this, it must also confer this lead authority the authority to investigate, impose fine, issue reprimand, order as well as notice for violations. This is to ensure a stringent and uniform application of the data protection regime, and avoid overlaps and inconsistent enforcement.

c. ***Dispute Resolution Mechanism***

Under the GDPR, the data subjects can address the processor and controller of their data in order to enforce their rights under the GDPR. With that being said, they can either lodge a complaint with the supervisory authority,[94] who will then investigate if an infringement had occurred, or lodge it with the judicial authority.[95]

The MoCI Regulation, on the other hand, only stipulates that a Director-General under the Minister to have jurisdiction to "receive the complaints of Data Subjects" (Article 30 paragraph (1)) and to create a dispute resolution panel.[96] The Owners of Personal Data can only bring complaint for failure of the Provider of Service (i.e. controller) to notify them or

---

87 Articles 52 paragraph (2) and 52 paragraph (4) of the GDPR, n.4.
88 Article 58 paragraph (1) of the GDPR, n.4.
89 Article 58 paragraph (2) letter (a) of the GDPR, n.4.
90 Article 58 paragraph (2) letter (c) of the GPDR, n.4.
91 Article 58 paragraph (2) letter (i) of the GDPR, n.4.
92 Article 58 paragraph (4) of the GDPR, n.4.
93 Article 36 paragraph (1) letter (c) of the MoCI Regulation.
94 Article 77 paragraph (1) of the GDPR, n.4.
95 Article 79 paragraph (1) of the GDPR, n.4.
96 Article 30 paragraph (2) of the MoCI Regulation

other Providers about security failure which may or may not cause damages,[97] or a tardy notification of such failure which caused damages.[98] The Owners may only bring judicial civil claim after the mandatory dispute settlement mechanism failed to bring about a peaceful resolution.[99]

This mandatory method of dispute settlement, a dependent supervisory authority, a very weak power granted to the Directorate-General and non-automatic right to judicial complaint make it very likely that the rights of the Owners will be effective, *vis-a-vis* big Providers of Service (i.e. controller), such as Facebook or Google who may have the capacity to fight a judicial complaint before a court. On this end, the Data Protection Bill should confer such right on the Owners of Personal Data so that they might exercise the rights endowed therein effectively, preferably with the help of a supervisory authority.

d. *Organisational Measures - the GDPR's Data Protection Officer*

The MoCI Regulation also merely obliges the Providers (i.e. Controller) to nominate a contact person whom the Owners of Personal Data (i.e. data subjects) may reach out regarding management of their personal data. This role seems to imitate that of Data Protection Officers ("**DPO**") which the GDPR mandates every Processor and Controller to nominate in Article 37; however, it must be noted that the role of the DPO is much more extensive than that of this contact person.

A DPO is supposed to monitor the implementation of the GDPR within the environment of their employer, counsel their implementation, and coordinate with the supervisory authority. They are to be the first contact for the data subjects.[100] To fulfill these duties, they are to be independent from instruction pertaining to their task in this field,[101] but they may also perform other duties granted it does not conflict with ones which pertain to data protection.[102]

As elaborated, the DPO does much more than a contact person. Consequently, it is highly recommended that the Data Protection Bill include a provision for such provision, in order to make an effective exercise of the rights of the Owners of Personal Data.

G. Conclusion

This article sets out to identify the different weaknesses within Indonesia's prevailing data protection regime. In doing so, it identified the different regulatory approach and solutions which the two entities followed.

This paper concludes that the Indonesian regime is severely wanting when compared to the GDPR. Next to this conclusion, this paper also offers its piece on the solution to these shortcomings, e.g. independent supervisory lead authority, a more expansive material scope, as well as a more structured approach to the enumeration of the rights and obligations of each player (i.a. the User, the Provider, and the Owner) to make identification of the rights and obligations of these players more easily identifies.

---

97 Article 29 paragraph (3) letter (a) of the MoCI Regulation
98 Article 29 paragraph (3) letter (b) of the MoCI Regulation
99 Articles 32 paragraph (1) & 32 paragraph (2) of the MoCI Regulation
100 Article 38 paragraph (4) of the GDPR, n.4.
101 Article 38 paragraph (3) of the GDPR, n.4.
102 Article 38 paragraph (6) of the GDPR, n.4.

BIBLIOGRAPHY

Books and Journals Articles

EU Transfers of data to UK post-Brexit: The GDPR perspective. (2018). International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel, 1.

Fielding, R. (2018). The Concept of Controller and Processor Data Entities, Int'l J. Data Protection Officer, Privacy Officer & Privacy Couns, 2, 1–13.

Lindroos-Hovinheimo, S. (2018). Who controls our data? The legal reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v Jehovan todistajat. Information & Communications Technology Law, 28(2), 225–238.

Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall L. Review, 47, 809.

Voigt, Paul. Von Dem Bussche, Axel. (2018). EU General Data Protection Regulation (GDPR): a practical guide. S.l.: Springer International Public International Law.

Legislations

Amended Indonesian 1945 Constitution

Commission Implementing Decision (Eu) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31

Indonesian Law No 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law

No 19 of 2016 Indonesian Government Regulation 82/2012 on Provision of Electronic System and Transaction

Indonesian Government Regulation 82/2012 on Provision of Electronic System and Transaction

Indonesian Ministerial Regulation 20/2016 on Protection of Personal Data of the Information Ministry

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) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 2

Treaty on Functioning of European Union

Jurisprudences

Judgment of the Court of 4 December 1974, Yvonne van Duyn v Home Office, Reference for a preliminary ruling: High Court of Justice, Chancery Division - United Kingdom, Case 41-74, ECLI:EU:C:1974:133

Judgment of the Court of 5 April 1979, Reference for a preliminary ruling: Pretura di Milano – Italy, Case 148/78, ECLI:EU:C:1979:110

Judgment of the Court of 17 September 2002, Antonio Muñoz y Cia SA and Superior Fruiticola SA v Frumar Ltd and Redbridge Produce Marketing Ltd, Reference for a preliminary ruling: Court of Appeal (England & Wales) (Civil Division) - United Kingdom, ECLI:EU:C:2002:497

Judgment of the Court of 6 November 2003, Criminal proceedings against Bodil Lindqvist, Case C-101/01, ECLI:EU:C:2003:596

Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI:EU:C:2014:317

Judgment of the Court (Fourth Chamber), 11 December 2014, František Ryneš v Úřad pro ochranu osobních údajů, Case C-212/13, ECLI:EU:C:2014:2428

Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650

Judgment of the Court (Grand Chamber) of 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, ECLI:EU:C:2018:388

Judgment of the Court (Grand Chamber) of 10 July 2018, Proceedings brought by Tietosuojavaltuutettu, C-25/17, ECLI:EU:C:2018:551

Miscellaneus

Kang, C., & Frenkel, S. (2018, April 4). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. Retrieved January 1, 2020, from https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html?action=Click&contentCollection=BreakingNews&contentID=66776835&pgtype=Homepage

The Value of Personal Online Data. (2018, April 23). Retrieved January 1, 2020, from https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data.

Rahma, A. (2019, December 19). Menkominfo: Draf RUU Perlindungan Data Pribadi Segera ke DPR. Retrieved 1 January 2020, from https://nasional.tempo.co/read/1285533/menkominfo-draf-ruu-perlindungan-data-pribadi-segera-ke-dpr/full&view=ok