Journal of Central Banking Law and Institutions, Vol. 2 No. 3, 2023, pp. 481 - 512
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
https://doi.org/10.21098/jcli.v2i3.171

DATA SUBJECT ACCESS REQUEST: WHAT INDONESIA CAN LEARN AND OPERATIONALISE IN 2024?

Muhammad Deckri Algamar,[a] Noriswadi Ismail,[b]

[a] Faculty of Law Universitas Indonesia, [b]European Advisory Board Member, International Association of Privacy Professionals, Indonesia, and United Kingdom
e-mail: deckrialgamar@gmail.com (corresponding author); e-mail: noriswadiismail1976@gmail.com

Submitted: 25 February 2023 - Revised: 28 July 2023 - Accepted: 28 August 2023

Abstract

The enactment of the Indonesian Personal Data Protection (PDP) Law is in line with the nation's position as the most promising digital economy in Southeast Asia. The PDP Law, amongst others, introduces Data Subject Access Request (DSAR), a cornerstone mechanism to exercise data subject rights mirroring the European Union General Data Protection Regulation (GDPR). However, major causes of DSAR failure are predominantly triggered by resource constraint, lack of fundamental understanding, and technical gap when responding to such requests. In practice, DSAR management is time consuming and taxing since organisations shall manage numerous and complex requests within a tight timeline. By way of comparative analysis, we explore the concept of data subject rights, specifically the Rights to Access. Through observations and constructive responses by global data protection professionals, academics and non-lawyers, this paper alluded that similar failure scenario might occur in Indonesia when PDP Law grace period ended in 2024 – if the causes are not addressed and mitigated. Apropos, in safeguarding data subjects' right, we assert that DSAR under the PDP law might bring disproportionate impracticality, hence there is demand for a robust consultation and holistic regulatory implementation. We also propose to consider a harmonized DSAR ASEAN framework for future proofing cross-border payment, in 2024 and beyond.

Keywords: *Data Protection, Cybersecurity, Financial Technology, Indonesia PDP Law, The EU GDPR, DSAR, ASEAN*

I. DEVELOPMENT OF INDONESIA PDP LAW AND THE EU GDPR

Privacy and personal data protection are two distinct but interrelated concepts. The term privacy was first proposed by Warren & Brandeis who argued that privacy is the right to be left alone and must be respected by law.[1] Privacy is further elucidated by David Banisar, who classified four different categories of privacy: 1) physical/bodily privacy; 2) territorial privacy; 3) communication privacy; and 4) informational privacy. Within that taxonomy, personal data protection is considered as part of informational privacy.[2] In order to ensure protection of an individual's informational privacy, data protection laws were created to govern how data is processed from the collection, recording, organising, storage, rectification, transfer, deletion, and up to data destruction.[3]

The transition from a traditional society to an information society has driven various technological developments, the rise of advanced gadgets and complex networks have augmented many activities in all layers of society.[4] In the realm of data processing, current technology enables real-time personal data collection of family members, user geolocation, transaction pattern, and other datasets that can be analysed for strategic and commercial purposes.[5] The growth also accelerated throughout the COVID-19 pandemic, that spurning technology adoption by society, companies, and government in delivering goods or services. However, this rapid development should be approached prudently, as technological benefits can also be used for malicious purposes through personal information theft, impersonation, and other cybercrimes that exist due to the lack of awareness of digital privacy and security.[6]

The incident of Facebook-Cambridge Analytica has become a stark reminder of the need to increase privacy awareness for users and for governments to review their data protection laws to prevent organisations from unlawfully processing data or exploiting its users. 87,000.000 Facebook users' data were collected without the user's consent and transferred to third parties that analysed and used the insight for political gains in various elections

---

* The views and analysis do not represent The International Association of Privacy Professionals but solely the author's.

1 Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review*, no. 5 (December 1890): 193-220.

2 David Banisar, "Privacy & Human Rights an International Survey of Privacy Laws and Developments," *The John Marshall Journal of Computer & Information Technology,* vol. XVIII (January 1999): 6.

3 Ian J. Lloyd, *Information Technology Law*, (United Kingdom: Oxford University Press, 2014), 52.

4 Edmon Makarim, *Pengantar Hukum Telematika* (Depok: PT Raja Grafindo Persada, 2005), 31.

5 Daniel J. Solove, *The Digital Person, Technology, and Privacy in the Information Age* (New York: New York University Press, 2004), 13.

6 Solove, *The Digital Person,* 13.

in the United States of America, South Africa, and the United Kingdom.[7] The aftermath of Cambridge Analytica has incentivised many countries to strengthen and/or revamp their data protection regulations to ensure better safeguards are available to its citizens. Such development has brought the EU GDPR which succeeds European Data Protection Directive 95/46/EC, as a control mechanism for data processing entities within the EU. There is no recognized binding standard on data protection, but international guidelines such as 1980 OECD Privacy Guideline was the first non-binding global framework to set minimum standard on the protection of privacy & data protection.[8]

As a primer, the EU GDPR is the pillar of data protection in the EU that aims to harmonise the national legislations of its member states. Interestingly, the EU GDPR is one of the regulations that experienced the "Brussels Effect," a term used to refer when an EU legislation has a direct or indirect effect on jurisdictions beyond the EU.[9] For instance, the extraterritorial effect of the EU GDPR has created a situation where US-based service providers must also comply with the EU GDPR as long as they offer services through data processing activities of EU dataset.[10]

In addition to being state-of-the art legislation on data protection, this development popularised concepts such as data processing principles, data actors (such as data subject, data controller, data processor), rights, and obligations among states outside of the EU. This is exemplified in jurisdictions that modelled their data protection laws on key GDPR concepts including the Brazil General Data Protection Law, the Singapore PDP Act**,** and the USA's California Consumer Privacy Act.[11] This connection is considered essential, especially in the context of international data transfers that prioritise adequacy conditions where both states have at least a similar or stronger data protection regulation.

---

[7] Jina Moore, "Cambridge Analytica Had a Role in Kenya Election, Too," The New York Times, March 20, 2018, https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html/; Paul Lewis and Paul Hilder, "Leaked: Cambridge Analytica's blueprint for Trump victory," The Guardian, March 23, 2018, https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trumpvictory/; Ed Power, "The Great Hack: The story of Cambridge Analytica, Trump and Brexit," The Irish Times, July 24, 2019, https://www.irishtimes.com/culture/tv-radio-web/the-great-hack-the-story-of-cambridge-analytica-trump-and-brexit-1.3965788.

[8] Graham Greenleaf, "Data Privacy Laws in Asia: Context and History," in *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, (United Kingdom: Oxford University Press, 2017), 9-10.

[9] Anu Bradford, "The Brussels Effect," *Northwestern University Law Review*, no. 1 (2015): 1–68.

[10] Christian Peukert et. al, "Regulatory export and spillovers: How GDPR affects global markets for data," *Centre for Economic Policy Research*, September 30, 2020, https://cepr.org/voxeu/columns/regulatory-export-and-spillovers-how-gdpr-affects-global-markets-data.

[11] Anastasia Petrova, "The Impact of the GDPR Outside the EU," *Lexology.com*, September 17, 2019, https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f.

Indonesia, as a developing country, has pursued stronger data protection law reform to accommodate the digital economic growth and offer a safer online environment. According to Sinta Dewi Rosadi, there are two main factors influencing the legal development of data protection law in Indonesia.[12] First, the existence of a human rights instrument enshrined under International Covenant on Civil and Political Rights, referred to under Indonesian 1945 Constitution as the right to live. Second, the rapid development of technology in Asia that has created a sense of urgency to provide better personal data protection. The ability of major technology industry to collect and analyse information has triggered complaints by consumers ranging from lack of digital trust to cyber-enabled criminal activities.[13]

The journey to shape data protection law in Indonesia has been challenging. Prior to 2022, the legal development was only sectoral and not unified into omnibus or comprehensive legislation.[14] For instance, data protection themes are reflected in Law No. 23 Year 2006 on Civil Administration, Law No. 29 Year 2004 on Medical Doctor Practices, Law No. 28 Year 2007 on Tax General Provision & Procedure, Law No. 19 Year 2016 on the Amendment of Information and Electronic Transaction. While on the level of implementation, there are Government Regulation No. 37 Year 2007 on the Implementation of Civil Administration, Law No. 71 Year 2019 on Electronic System and Transaction Operations, and Law No. 80 Year 2019 on Electronic Commerce. As a consequence of this fragmented and sectoral approach, several sectors may have no data protection themes at all or regulatory arbitrage with different data protection interpretations. Due to this landscape, the need to create a comprehensive data protection law is timely.

In 2022, Law No. 27 Year 2022 on Personal Data Protection came into force.[15] This was a pivotal moment for the Indonesian government to commit to better protection for its citizens' personal data and as a response to high-risk cyber-attacks that threaten the integrity, confidentiality, and availability of data. The law aspires to increase awareness and legitimacy of data protection

[12] Sinta Dewi, "Balancing Privacy Rights and Legal Enforcement: Indonesia Practices," *International Journal of Liability and Scientific Enquiry* 5, (February 2012): 233, https://doi.org/10.1504/IJLSE.2012.051961.

[13] Sinta Dewi Rosadi, Siti Yuniarti, and Rizki Fauzi, "Protection of Data Privacy in the Era of Artificial Intelligence in the Financial Sector of Indonesia," *Journal of Central Banking Law and Institutions,* no. 2, (2022): 353-366, https://doi.org/10.21098/jcli.v1i2.18.

[14] Jeferson Kameo, "Panama Papers dan Diskursus tentang Perlindungan Data di Indonesia: Suatu Perspektif Teori Keadilan Bermartabat," *Jurnal Refleksi Hukum,* no. 1, (2016): 92, https://doi.org/10.24246/jrh.2016.v10.i1.p84-98.

[15] Ima Dini Shafira, "DPR Resmi Sahkan RUU Perlindungan Data Pribadi," *Tempo.co*, September 20, 2022, https://nasional.tempo.co/read/1636301/dpr-resmi-sahkan-ruu-perlindungan-data-pribadi.

to all actors.[16] Indonesian Constitutional Court also recognises personal data protection as part of human rights in the technologically advanced era to ensure individual rights throughout personal data processing are adequately protected and provides trust to the society.[17] Promisingly, Law No. 27 Year 2022 on Personal Data Protection marks a new era that will affect how organisations process personal data.

The Personal Data Protection Act (PDP) governs various aspects of data protection, including the classification of personal data, data subject rights, personal data processing, obligation of data controllers and processors, international and national data transfer, the data protection supervisory authority, administrative and penal sanction, international participation, and the applicable procedural rules. The majority of these components are partly modelled upon the EU GDPR. This is not surprising since the draft of Indonesian Personal Data Protection Law was drafted with the EU GDPR as baseline reference, aimed to ensure that Indonesia might level up its protection, aligned with the EU GDPR, subject to several exceptions.[18] Owing to this, legal scholars have extensively discussed topics under the EU GDPR as contextually relevant *vis-à-vis* PDP Law and its future development.

Despite bringing tremendous benefits to both consumers and business, the EU GDPR has also brought unintended consequences – one of which is the burdensome compliance costs of organisations that process personal data.[19] Previously, Wanda Preshtus & Kaja Felix have classified and ranked failures to act on data subject rights to be one of the most frequent five violations of data protections laws.[20] In combination with unclear implementation guidance for various requirements, the International Association of Privacy professionals (IAPP)-EY Privacy Governance Report revealed that many business operations have failed to comply with the regulations after they came into effect in 2018.[21]

---

[16] Umi Sugiyanti and Agung Pambudi, "Perlindungan Data Privasi dan Kebebasan Informasi dalam Platform WhatsApp," *Jurnal Ikatan Pustakawan Indonesia*, no. 2 (2022): 67.

[17] Indonesian Constitutional Court, Decision number 108/PUU-XX/2022, pp. 117-118; Danrivanto Budhijanto, "Cybersecurity dan Hukum Pelindungan Data Pribadi di Indonesia," in *Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity*, (Bandung: Refika Aditama, 2023), 65.

[18] Pratiwi Agustini, "UU PDP Akan Permudah Pertukaran Data dengan Negara Lain," *Direktorat Jenderal Aplikasi Informatika,"* accessed January 21, 2023, https://aptika.kominfo.go.id/2020/11/uu-pdp-akan-permudah-pertukaran-data-dengan-negara-lain/.

[19] Eline Chivot and Daniel Castro, "The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy," *Center for Data Innovation,* May 13, 2019, https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/.

[20] Wanda Presthus and Kaja Felix Sønslien, "An analysis of violations and sanctions following the GDPR," *International Journal of Information Systems and Project Management*, no. 1 (2021): 45-46, https://doi.org/10.12821/ijispm090102.

[21] "IAPP-EY Annual Privacy Governance Report 2018," International Association of Privacy Professionals and Ernst & Young, accessed January 21, 2023, https://iapp.org/resources/article/iapp-ey-annualgovernance-report-2018/.

Indonesia is not an exception. Certain sectors have voiced out their concerns on the Indonesian PDP Law enforcement that might pose significant compliance risk and become a barrier to innovation.[22] However, the Indonesia PDP Law has yet to become effective (slated for 2024) and requires further implementing regulatory details, which are currently being drafted. This specific context triggered a perfect timeline to delve further into the normative obligations contained in the law and if additional adjustments are needed. Therefore, this paper builds upon the latter toward balanced academic and practical analysis.

Within the context of the data protection regime, there are four main actors that are actively involved. First, the data subject whose personal data is processed such as the active user of an application. Second, data controller is an entity that acts separately or jointly with other data controllers to determine the purpose of data processing (in many instances, data controller is also the actor who offers products/services to the consumer/data owner). Third, a data processor appointed by data controller to help the latter in processing collected data. Lastly, there are third parties not directly linked with the product/services.[23] Depending on its business model and how data is processed, many Financial Technology companies can be contextually categorised as data controllers or data processors or both.[24]

This paper will be the first to discuss data subjects' rights, and particularly the exercise of data subject access request ("DSAR") within an Indonesian context, supplemented by the EU GDPR-style. We start this paper by introducing the developments of personal data protection in Indonesia and how other jurisdictions have influenced the existing law. The issue is particularly important due to potential challenges the industry may face in complying with the strict deadline of DSAR.[25] We dissect the importance of data within the Financial Technology (Fintech) industry and why compliance with data protection laws is essential. Subsequently, we explore DSAR in the context of Indonesian law while proposing how implementing regulations should be structured to reflect international best practices. We also provide

[22] Yudha Pratomo, "Google Sebut UU Perlindungan Data Pribadi Bisa Menyusahkan Startup," *Kompas.com*, August 28, 2019; https://tekno.kompas.com/read/2019/08/20/14050087/google-sebut-uu-perlindungan-data-pribadi-bisa-menyusahkan-startup?page=all; Lona Olavia, "Industri Minta Kepastian Hukum Perlindungan Data Pribadi," *BeritaSatu.com,* March 30, 2021, https://www.beritasatu.com/ekonomi/753123/industri-minta-kepastian-hukum-perlindungan-data-pribadi.

[23] Thomas Linden et al., "The Privacy Policy Landscape After the GDPR," *Proceedings on Privacy Enhancing Technologies,* no. 1 (2020): 48-49, https://doi.org/10.2478/popets-2020-0004.

[24] Kazim Degerli, "Regulatory Challenges and Solutions for Fintech in Turkey," *Procedia Computer Science* 158 (2019)*:* 935.

[25] Andre Soelistyo, "UU PDP & Kepatuhan Industri," *Bisnisindonesia.id.*, October 6, 2022; https://bisnisindonesia.id/article/opini-uu-pdp-kepatuhan-industri.

a case study of QRIS DSAR and point out at least three concerns on the current national and regional regulations for access request and reflect on other Fintech companies' readiness to handle DSAR.

In relation to data subject rights, there has been literature identifying data subject rights within the EU GDPR and the Indonesian PDP Law. Helena Vrabec has identified data subject rights in the context of the digital economy,[26] while Ausloos & Dewitte have examined DSAR and its subsequent cybersecurity impact within the EU jurisdiction.[27] In understanding the Indonesian context, there have been various data protection scholars writing *a priori* to the Indonesian PDP Law but no specific coverage and deep dive analysis relating to DSAR. We acknowledge and refer to these indispensable legal scholars from two jurisdictions to provide greater clarity on how the Indonesian PDP Law should proceed with DSAR implementation.

We substantiated and balanced our research by conducting a DSAR Awareness Survey on 7 February and was opened after the presentation of this paper in Bali, May 2023. As of the 21st of April, 95+ respondents, ranging from global privacy practitioners, academia, organisations, and students have participated. The questionnaire highlights five important insights on DSAR; 1) The familiarity of DSAR; 2) The procedures of DSAR; 3) Automating DSAR; 4) Indonesian 3x24 hours DSAR timeline; and 5) Input for Indonesian DSAR timeline. Aside from multiple choice, we provide an option for respondents to provide pragmatic insights. We combine theoretical applications derived from the literature review together with DSAR Awareness Survey to objectively unbox DSAR's complexity in practice.

II. DATA SUBJECT RIGHTS IN FINANCIAL TECHNOLOGY: A NEW HORIZON FOR COMPLIANCE IN A DIGITALLY DRIVEN ECONOMY

Within the financial sector, innovation and digital transformation is key to producing seamless delivery service to customers through trusted online customer's journey and experiences throughout the COVID-19 pandemic. The financial sector faced substantial challenges that incentivised changes, leading to a rapid rise of Fintech services' subscriptions and activities. [28] At the time, Indonesia experienced massive growth in Fintech companies such as Ajaib,

[26] Helena Vrabec, *Data Subject Rights under the GDPR with a Commentary Through the Lens of Data-Driven Economy* (New York: Oxford University Press, 2021), 38.

[27] Jef Ausloos and Pierre Dewitte, "Shattering One-Way Mirrors. Data Subject Access Rights in Practice," *International Data Privacy Law* 8, (2018): 30.

[28] Keke Gai, Meikang Qui, Xiaotong Sun, "A survey on FinTech," *Journal of Network and Computer Applications*, vol. 103 (2018): 262–273.

Xendit, Akulaku, and 100+ companies listed under the Indonesian Financial Service Authority with a total of US$20.4 billion funds to deliver. Fintech industry revolves around four main categories: (1) Payment, clearing, and credit settlement; (2) Deposit, lending, fundraising; (3) Market provisioning; and (4) Investment risk management that provides opportunities for Micro, Small, and Medium-Sized Enterprises.[29]

Fintech companies process voluminous personal data on their platforms including but not limited to profiling, targeting and analysing customers' datasets for revenue generation and improved future revenue generation models. The dataset is analysed according to the company's customised business model, such as planning new services or innovating future and improved products.[30] Hendrawan Agusta pointed out that in peer-to-peer lending Fintech, there are at least three sets of data collection.[31] First, financial data such as the amount of money invested, transaction history, maturity of loan repayments, and many others that are considered sensitive/special category data. Second, health and biometric data are collected when users upload photos of themselves, facial characteristics, and fingerprints to establish login credentials or authentication factors. Additionally, certain data are recorded by Fintech companies for mandatory customer onboarding, such as "Know-Your-Customer" verification methods as required by law.[32]

The voluminous dataset Fintech companies process might lead to cybersecurity risk exposure if security controls, and resilience are vulnerable. Hackers have a strong incentive to steal financial information, impersonate user transactions, and other illegal activities.[33] This puts tremendous burden on Fintech companies to ensure customers' personal data is protected and prevent cybersecurity threats. Hence, an introduction to data protection regime is necessary to protect its users.[34]

Previously, the Fintech sector faced regulatory limbo before the Indonesian Financial Service Authority stepped up through POJK No. 77/POJK.01/2016,

---

[29] Lastuti Abubakar and Tri Handayani, "Financial Technology: Legal Challenges for Indonesia Financial Sector," *IOP Conf. Series: Earth and Environmental Science* 175, (2018): 3.

[30] Elena Hernández et al., "Data Protection on Fintech Platforms," *International Conference on Practical Applications of Agents and Multi-Agent Systems*, vol. 1047 (June 2019): 223–233, https://doi.org/10.1007/978-3-030-24299-2_19.

[31] Hendrawan Agusta, "Keamanan dan Akses Data Pribadi Penerima Pinjaman dalam Peer to Peer Lending di Indonesia," *KRTHA Bhayangkara*, no. 1 (June 2021): 18-19, https://doi.org/10.31599/krtha.v15i1.289.

[32] Arnoud Boot et al., "Fintech: what's old, what's new?" *Journal of Financial Stability* 53, (2021): 3*, https://doi.org/ 10.1016/j.jfs.2020.100836*.

[33] Aleksandr P. Alekseenko, "Privacy, Data Protection, and Public Interest Consideration for Fintech," in *Global Perspectives in FinTech: Law, Finance and Technology,* (London: Palgrave Macmillan, 2022), 39.

[34] Alekseenko, "Privacy*,"* 27.

IT-Based Lending & Borrowing Services. Under Article 21, it sets out several obligations of Fintech companies to minimise risk against its customers but does not specifically regulate the use of personal data.[35] Afterwards, the Central Bank of Indonesia (Bank Indonesia) published Fintech regulations – in which it defines Fintech as "the use of technology within a financial system that results on a novel product, service, technology, or business model" under Bank Indonesia Regulation 19/12/PBI/2017 on Financial Technology Implementation to ensure Fintech adherence on consumer protection, risk management, and security principles. Within Article 8 of this Regulation, all Fintech providers are obliged to ensure data confidentiality related to financial transactions. [36]

The Fintech business and technology model is progressive, seamless, and disruptive compared to traditional financial business model. In such circumstances, it should also comply with various regulations enforced by the Financial Service Authority, Bank Indonesia, and data protection as part of its compliance obligations. A privacy-respectful approach is important to balance the business interest of companies and the protection of customers' data. For example, end-to-end data encryption, increased or multi-layered authentication and secured networks. Given the Fintech landscape and progress in Indonesia, the following sections outline DSAR principles, processes, and practicalities, and equally how and why it is indispensable for Fintech companies to comply with such requests, post enforcement of the Indonesia PDP Law.

III. RIGHT TO ACCESS: CORNERSTONE MECHANISM FOR DATA PROTECTION

The Right to Access, which is ensconced in the DSAR, is one of the primary pillars of enforcement other data subject rights under the data protection law regime. Helena classified data subject rights into three categories: 1) Rights related to information & access to personal data; 2) Rights related to rectification & erasure of personal data; and 3) Rights to object against automated decision-making.[37] In relation to the first category, both Rights to Information & Rights to Access are considered to be cornerstones of exercising other rights as it's impossible for data subjects to request for rectification or even object to automated processing if they do not know the information that is being processed by the data controller.

---

[35] Abubakar and Handayani, "Financial Technology," 3.

[36] Indonesia, Bank Indonesia Regulation No. 19/12/PBI/2017 on Financial Technology Implementation, Article 8.

[37] Helena Vrabec, *Data Subject Rights under the GDPR with a Commentary Through the Lens of Data-Driven Economy* (New York: Oxford University Press, 2021), 38.

In practice, Rights to Access provides two main primary functions e.g., increasing transparency for data subject and acting as control mechanism against unlawful processing.[38] In support of Kranenborg's argument, the clarity and transparency over how data is processed are important for an individual.[39] Therefore, there is an emphasis to ensure that DSAR can be requested by data subjects and data controllers' commitment to these rights due to the high deference it holds in data protection regulations.

In the 2010s, Max Schrems's notable DSAR to Facebook led to ground-breaking litigation over Facebook's unlawful data processing activities that might have infringed on the EU GDPR. Max Schrems submitted DSAR and received a 1200-page long document that contained voluminous personal data. The list includes all his private messages, records of all "Like" activity, and many others which became the basis of 22 complaints directed to supervisory authorities to investigate Facebook's data protection compliance.[40] Max Schrems was not alone. Another DSAR leading to high-level investigation was requested by David Caroll that exposed Cambridge Analytica's conduct during the 2016 US President election.[41] These highlight the importance of acknowledging data subjects' DSAR rights and data controllers' obligations to comply with such requests. It must not be understated as failure to respond will lead to administrative fines and unsolicited access may hamper data controllers' trust and reputations.

Prior to the EU GDPR, Rights to Access could be referred to Article 12(a) of Data Protection Directive (DPD) 95/46/EC which mandates all EU member states to guarantee data subjects to have the ability in: (1) Confirming if personal data is being processed, and further detailing this processing activity; (2) Receiving communication in an intelligible form of personal data that is currently processed; and (3) Being informed if the processing is automated and the logic behind it.[42] However, since DPD 95/46/EC mandates member states and requires national legislation in transposing the Data Protection Directive, there has been substantial differences between member states in enforcing

[38] Gabriela Zanfir-Fortuna, "The EU General Data Protection Regulation (GDPR): A Commentary,": 452.

[39] Steve Peers et al., *The EU Charter of Fundamental Rights: A Commentary* (Oxford: Hart Publishing, 2014), 254.

[40] Hannah Kuchler, "Max Schrems: the man who took on Facebook - and won," *The Irish Times,* April 5, 2018, https://www.irishtimes.com/business/technology/max-schrems-the-man-who-took-on-facebook-and-won-1.3451485.

[41] Cedric Lauradoux, "Can Authoritative Governments Abuse the Right to Access?" in Privacy Technologies and Policy 10th Annual Privacy Forum, APF 2022 Warsaw, Poland, June 23–24, 2022, Proceedings, (Warsaw: APF 2022, 2022), 23.

[42] Gabriella Zanfir Fortuna, the EU General Data Protection Regulation (GDPR): A Commentary: 453.

and facilitating rights to access.[43] Due to this, the EU GDPR harmonises the modalities, deadlines, and mechanisms for handling Rights to Access across the EU member states.

In contrast to the EU, previous legislation related to data protection in Indonesia does not recognise Rights to Access of personal data by data subjects. Previously, Rights to Access only refers to the ability of government officials to access citizenship data for administrative purposes.[44] Therefore, Rights to Access by data subjects was newly introduced under the Indonesia PDP Law alongside other data subject rights under Chapter IV Article 5-14. Specifically, Article 7 states that *"Data Subjects shall have the right to access and obtain a copy of Personal Data regarding themselves in accordance with provisions of laws and regulations."*[45]

From the construction of Article 7, the Indonesian, PDP Law does not provide further corroboration regarding the scope of access provided to data subject, form of copy that will be given, nor the mechanism in providing access. This question remains open to further implementing regulations, as indicated in the last sentence of Article 7. This marks a significant departure of the Indonesian PDP Law from the EU GDPR in which the rights to access must not be interpreted narrowly as the rights to receive a copy. It is accepted that it must also cover additional set of information related to the request to ensure the requestor understands the context.[46]

The European Data Protection Board (EDPB) Guideline 01/2022 also reflects this position, by explicitly mentioning that obtaining a copy is not a separate right from Rights to Access, rather, access to copy and additional documents becomes the modalities or means of fulfilling the Rights to Access. The EDPB, as a European Union-level institution, has actively set out guidelines pertaining to GDPR Articles to ensure uniformed application and interpretation throughout member states. Although the Guidelines is not binding, it has been consistently followed by member state-level data protection authorities. Specifically, EDPB published Guidelines 01/2022 on Data Subject Rights - Rights to Access ("Guideline 01/2022"). Several topics discussed including: (1) General purpose & aim of the access; (2) Principles of the rights; (3) Scope of the rights; (4) How to provide access; and (5) Limits &

---

[43] Antonella Galetta et al., "Mapping the Legal and Administrative Frameworks of Access Rights in Europe: A Cross-European Comparative Analysis," Work Package 5 for the IRISS Project (2014).

[44] Article 79 of Law No. 23 of 2006 on Citizen Administration (Amended by Law No. 24 Year 2003).

[45] Article 7 of Law No. 27 of 2022 on Personal Data Protection Act.

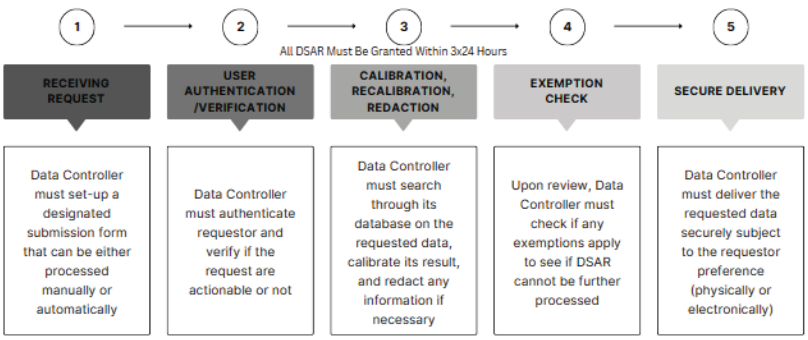
[46] Beatriz Esteves, Victor Rodriguez-Doncel, and Ricardo Longares, "Automating the Response to GDPR's Right of Access," *Legal Knowledge and Information Systems* (2022): 171, https://doi.org/10.3233/FAIA220462.

restrictions of Rights to Access.[47] From a practitioners perspective, Brennan & Matheson pointed that these Guidelines are vital to reflecting the views of data protection supervisory authorities and help organisations familiarise with the procedure to handle DSAR.[48]

III.A Data Subject Access Request in Practice

As the Indonesian PDP Law implementing regulations are still in the drafting phase, we propose five steps as set out in (Table 2). This flowchart is inspired by international best practices, partly replicating the EU GDPR-style practicalities.

Table 1. DSAR Workflow



III.A.1. Receiving Request

In practice, there are two options used by an organization to receive DSAR. First, DSAR can be submitted manually through email and processed via batches by an organisation's designated Data Protection Officer (DPO). Second, DSAR can be managed automatically.[49] Most DSAR are submitted through electronic means via an online form. This is consistent with the EU GDPR Recital 65 recommendation, which states that "[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data."[50] Based on our cursory review of leading Indonesian Fintech companies' privacy policy and privacy notice, we learned that some organizations have yet to designate a DPO, in the event there's future DSAR request from data subject. Push forward in

[47] "Guidelines 01/2022 on data subject rights - Right of access," European Data Protection Board, adopted on January 18, 2022, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

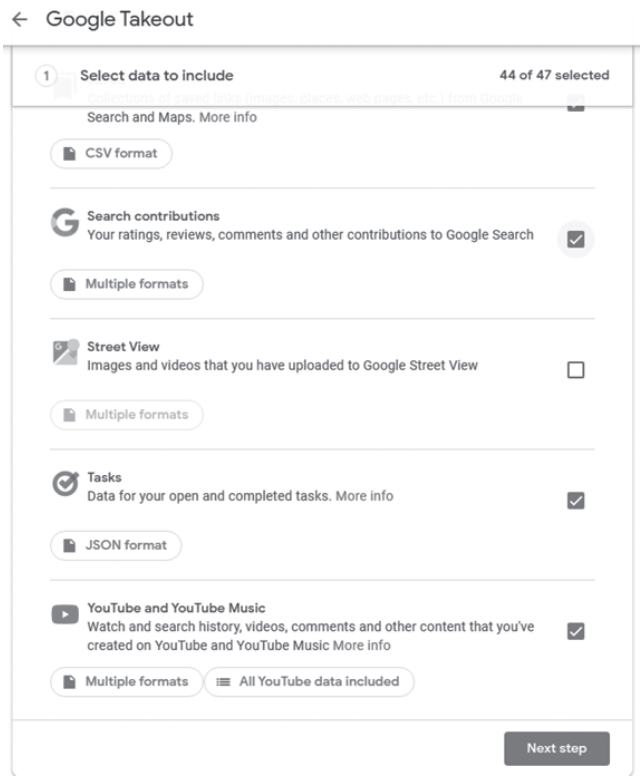
[48] Davinia Brennan, "The New Guidelines on Access Request – is the bar now too high?" *Data Protection Ireland,* vol. 15 (May 2022).

[49] Lauradoux, "*Can Authoritative*," 25.

[50] Vrabec, "*Data Subject,"* 38.

2024 and beyond, we assert and anticipate that it might change – subject to the Indonesian PDP Law enforcement and clear implementing regulations in place.

Image 1. Google Takeout Dashboard



The high frequency of DSARs submitted to an organisation has suggested that automation tools have become highly preferable. For instance, the use of a "Dashboard" format, at which users can request access through clicking options available in the setting menu. For example, *takeout.google.com* allows data subjects to select and choose categories of personal data being processed, whether the personal data will be sent at an interval, and the company will send out accordingly within 1-2 days.[51] The Dashboard is an optimal measure to verify data subject even before a request has been submitted.[52] Interestingly, 58.3% of respondents in our DSAR Awareness Survey revealed that they prefer the use of automated tool when handling DSAR – although several

[51] Google, "Google Takeout", https://takeout.google.com/.

[52] Thomas J. Smedinghoff, "The Duty to Verify Identity: A Criticial Component of Privacy and Security Compliance," *PLI 22nd Annual Institute on Privacy & Cybersecurity* (April 2021): 10.

comments partly suggested human input and intervention is pertinent (as and when necessary) while deploying automation tool.[53]

While the Dashboard option seems ideal, there are two main drawbacks. First, a data subject does not necessarily need to have an account to request access (for instance, IP collection and geolocation without a user account). Second, the use of a dashboard may not cater to a user's specific requests whilst the purpose and nature of DSAR is processed automatically as it might fail to provide a user with accurate information compared to manually responding to a request.[54] To mitigate potential drawbacks, Starling Bank, one reputable global Fintech company, has provided two options: manual request through a designated email and request through an application interface.[55] These options provide data subject an opportunity to opt.

The Indonesian PDP Law has yet to set forth specific step-by-step guidance on how data subjects can exercise DSAR or for data controller in handling such requests as Article 14 of the Indonesian PDP Law only clarifies that a request must be submitted electronically or manually.[56] In contrast, the EU GDPR amongst others, provided the modalities such as format of communication, readability of information given to users. While the Indonesian law is silent on modalities for managing DSAR. It is hoped and ideally anticipated that the Indonesian PDP law implementing regulations shall provide practical clarity in its future private and public consultations.

III.A.2. User Authentication or Verification

III.A.2.i. Methods in Verifying Data Subject Access Request

Recital 64 of the EU GDPR called out identity verification, indicating that "[t]he controller should use all reasonable measures to verify the identity of a data subject … a controller should not retain personal data for the purpose of being able to react to potential requests." It emphasises two important aspects: 1) The obligation to properly verify users; and 2) The limitation imposed against verification. In essence, Recital 64 provides leeway to data controller to adopt verification technique whilst verifying a requestor. Data controllers may ask for login credentials, email address, national identity card, home address, or even go as far as to call a data subject to properly authenticate the request before proceeding with the request.[57]

---

[53] Muhammad Deckri Algamar and Noriswadi Ismail, "*DSAR Awareness Question Survey Results":* Question 5, 2022.

[54] Vrabec, "*Data Subject,"* 110.

[55] Starling Bank. "Privacy Notice" Security Boulavard, Version 3.1, Effective 13 July 2022. https://www.starlingbank.com/legal/privacy-notice/

[56] Article 14 of Law No. 27 of 2022 on Personal Data Protection.

[57] Mariano Di Martino et al., "Personal Information Leakage by Abusing the GDPR ``Right of Access"," *Fifteenth Symposium on Usable Privacy and Security,* (August 2019): 374.

Data controllers should exercise precautionary measures such as requesting an ID Card as means of authentication, which may be considered not proportional. In short, the principle of data minimisation must always be upheld by requiring minimum information. As illustrated in the Irish Data Protection Commission Annual Report 2021, authentication through official ID is likely proportional only when it is impossible to determine the requestor's identity or he/she asks for sensitive data.[58] This stance is echoed in Guideline 01/2022 that explains the utilisation of ID Cards in verifying data subjects' identities can lead to unauthorised or unlawful processing by the data controller – even more so when the documents are stored by the data controller.[59]

Daniel Cooper & Lars Lensdorf pointed out that Guideline 01/2022 would place a considerable risk on data controllers, as it did not provide a solution on how to verify request where verification is needed or when requesting certain document would not be proportional. Alongside other commenters, Cooper & Lensdorf proposed that requesting ID Cards for verification should be allowed if: 1) There is a reasonable doubt on the identity of requestor; or 2) Requesting party has not been authenticated through login credentials. [60] A more stringent verification system is needed to prevent misidentification which would result in personal data leaks to unauthorised parties.

The duty to verify, consistently applies even if no personal data has been disclosed by a data controller. This is illustrated in the financial penalty given to Telecom GmbH for failing to set out strong identity verification measures, where a person could receive personal data by only providing name and date of birth.[61]

The Indonesian PDP Law omits any norms for verifying data subjects' requests that might cause an assumption that verification is not necessary. This is deeply concerning, as responding to DSAR must be done carefully as the information contained (and to be shared) may be sensitive and a false requestor becomes a risk that cannot be understated.[62] The term "verification" is called out in Article 29 that mandates data controllers to carry out verification to

---

[58] Data Protection Commission, "Irish Data Protection Commission's Annual Report 2021," *An Coimisiun Chosaint Sonrai,* February 24, 2022, 30.

[59] European Data, "Guideline 01/2022," 69-78.

[60] Daniel Cooper & Lars Lensdorf, "EDPB Draft Guidelines 01/2022 on Data Subject Rights – Right of Access", *Computer Law Review international* (March 2022): 68.

[61] Graham Cluley, "1&1 Telecom GmbH hit by almost €10 million GDPR fine over poor security at call center," *Security Boulavard,* last modified December 11, 2019, https://securityboulevard.com/2019/12/11-telecom-gmbh-hit-by-almost-10-million-gdpr-fine-over-poor-security-atcall-centre.

[62] Vrabec, "*Data Subject,"* 111.

ensure accuracy, completeness, and consistency of personal data.[63] However, according to the Article, it is unlikely that this obligation refers to the act of verifying data subjects' access requests since it puts no reference on data subject rights. Therefore, the Indonesian PDP Law is noticeably weak in governing the handling data subject requests from the lens of verification.

Outside of the data protection context, the duty to verify is a requirement in Anti Money Laundering regulations, Bank Indonesia and Otoritas Jasa Keuangan regulations. For instance, Article 19 of Bank Indonesia Regulation No. 23/15/PBI/2021 on Central Bank Services regulates cautionary principle implementation in the form of identification, verification, and monitoring as part of customer due diligence is under Financial Service Authority Regulation No. 23/POJK.01/2019 on AML & Terrorism Funding Prevention.[64]

Article 17 provides mandatory *know-your-customer* programmes which require the submission of National ID.[65] While this is an example of documents used to verify customers' identities, it cannot be automatically translated as the necessary documents for DSAR from data subjects – as not every request requires stringent verification. For instance, the Spanish Data Protection Authority fined a company for requesting ID, electricity bills, and insurance cards to verify DSAR requests on data subjects already registered.[66] Therefore, the implementing regulations for the Indonesian PDP Law need to clarify types of documents to consider proportionality for each request.

III.A.2.ii. Should 3x24 Hours Time-Limit Starts Before Authentication Process?

One of the most common violations regarding DSAR, is the failure to provide timely responses. In relation to DSAR timeline, there is a noticeable difference between the EU GDPR and Indonesian PDP Law. Under the EU GDPR, Article 12 stipulates "controller shall provide information on action taken on a request … without undue delay, and in any event within one month of receipt of the request." This deadline applies to most data subject rights such as Rights to Access (Article 15), Rights to Rectification (Article 16), Rights to Erasure (Article 17), Rights to Restriction of Processing (Article 18), Rights to Data Portability (Article 20), Rights to Object (Article 21), Rights to Not be Automatically Processed (Article 22), and in addition: the Rights to be Notified in Case of Rectification and Erasure (Article 19). One must note that

[63] Indonesia, Law No. 27 of 2022, Personal Data Protection, Article 29.

[64] Indonesia, Bank Indonesia Regulation No. 23/15/PBI/2021 on QRIS Standard Implementation, Article 19.

[65] Indonesia, Financial Service Authority Regulation No. 23/POJK.01/2019 on AML & Terrorism Funding Prevention, Article 17.

[66] Alan Tang, *Privacy in Practice: Establish and Operationalize a Holistic Data Privacy Programme*, (Abingdon: CRC Press, 2023) p. 398.

the deadline under Article 12 does not mean the rights must be fulfilled within a certain period, as it only mandated the data controller to provide any forms of response regarding information of the submitted request.

Prior to Guideline 01/2022, Helena Krabec pointed out that there are two diverging interpretations on when the timeline begins. First, several data protection authorities have strictly followed the "date of receipt" wording of the EU GDPR where the date will be counted from when the request is received. On the other hand, other data protection authorities have followed a more flexible approach by counting "date of receipt" after a qualified request – meaning after the request is clarified, paid, or where the requestor has been successfully verified.[67] However, guidelines under 01/2022 provides clarity that the time limit should start when the request reaches the controller (regardless of whether the controller is aware or not) but can be suspended if there is uncertainty regarding the requestor identity or when the data controller requires additional information regarding specificity of the request.[68] On that note, EDPB also recommends for data controllers to send out confirmation on the request's receipt and informs the data subject on specific timeline (e.g.: the one month period from 20 January 2023 to 20 February 2023).[69] Therefore, there is clarity on the time limit.

In Indonesia, the time limit for exercising data subject rights is tabulated below:

Table 2. Data Subject Rights Timeline

No.	Issue	Legal Basis	Deadline
1.	Right to rectify	Article 30	3x24 hours (3 days) after receiving a request
2.	Right to access	Article 32	3x24 hours (3 days) after receiving a request
3.	Right to object	Article 40	3x24 hours (3 days) after receiving a request
4.	Right to restriction of processing	Article 41	3x24 hours (3 days) after receiving a request

Similar to the EU GDPR, the Indonesian PDP Law has set out a uniformed time limit to respond to data subject rights. Interestingly, the wording leads to completion of the request – not a response to the request. For instance, Article 32 Paragraph (2) stipulates "[t]he access as referred to in paragraph (1) **shall be granted** no later than 3 x 24 (three times twenty-four) hours from the time that the Personal Data Controller receives the access request." This is a stark difference from the time limit provided under the EU GDPR which

[67] Vrabec, "*Data Subject,"* 113.
[68] European Data, "Guideline 01/2022," 157.
[69] European Data, "Guideline 01/2022," 57.

requires that "[t]he controller shall **provide information on action taken on a request** under Articles 15 to 22 to the data subject … in any event within one month …" Therefore, Indonesian data protection laws expect the request to be fulfilled within 72 hours while the EU GDPR only requires any forms of response within one month of the receipt.

The time limit for DSAR will become a huge issue in Indonesia if Article 32 Paragraph (2) is not amended or further clarified in its implementing regulation. Previously, Asosiasi Fintech Indonesia (AFTECH) submitted its input on the draft of Indonesian PDP Law and discussed with the Indonesian Parliament regarding several issues in the draft. Timeline for right to access is a contentious issue. AFTECH viewed the time limit as extremely restrictive based on two rationales: 1) Not all industries have the same capacity to comply with 3x24 hours timeline; and 2) The proposed timeline are stricter than the EU GDPR (one month with possible extension) and even the Malaysia Personal Data Protection Act 2010 (21 days with possible extension).[70]

Other jurisdictions, such as the California Consumer Privacy Act, allow up to 45 days with possible extensions in responding to DSAR.[71] While the Singapore Personal Data Protection Act of 2012 sets out an obligation to provide access as soon as possible, but allows extension by the company if it unable to provide access within 30 calendar days after notifying the requestor.[72] This shows that Indonesia is on the extreme side in DSAR time limit, as well as DSAR completion date.

According to Meribeth Banaschik, DSAR compliance is not easy. From a resource perspective, it would require around US$ 1400 for each company to set out a system to handle DSAR exercise effectively while manual DSAR would require approximately two weeks to be processed.[73] This is consistent with our survey result, to which a short DSAR timeline is suboptimal with 50% views that they are unsure if meeting the deadline is possible and 20.83% views it is not possible. Of relevance and to contextualize, Fintech companies might face problems in compiling high volume DSAR within such strict deadlines.

---

[70] "Masukan dan Pandangan Industri Fintech atas Rancangan Undang-Undang Perlindungan Data Pribadi," Fintech Indonesia: 50, accessed on 5 February 2023 https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200706-021940-3243.pdf; Rancangan Undang-Undang Data Pribadi," Fintech Indonesia: 18, accessed on 5 February 2023, https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200706-022052-5497.pdf.

[71] "The California Consumer Privacy Act of 2018," Spirion: 1798.130, accessed on 7 February 2023, https://www.spirion.com/wp-content/uploads/2020/07/Spirion_CCPA_v3.pdf.

[72] "Guide to Handling Access Requests," Personal Data Protection Commission Singapore, accessed on 7 February 2023, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-handling-access-requests-v1-0-(090616).pdf.

[73] https://www.ey.com/en_gl/forensic-integrity-services/how-to-comply-with-data-subject-access-request.

III.A.2.iii. Risk Related to Deadlines and Incorrect Verification

Within the context of DSAR deadline, organisations are being pressured into adhering to two aspects. First, the obligation to fulfil data subject's rights within a strictly imposed timeline. Second, it must manage DSAR prudently as to prevent any unauthorised disclosure to another party. However, the two obligations can conflict with each other if organisations bypass security measure that might infringe the Rights to Access through unauthorised third parties' unlawful data access. In 2018, Pavur and Knerr conducted a study of 150 companies on attempts to simulate access requests from hackers by utilising publicly accessible data to bypass DSAR verification mechanisms. Unclear DSAR implementation guidelines and weak authentication obligation to data controllers might lead to dreadful penalty. For instance, data subjects are compelled to refuse providing additional documents by arguing that it is not "proportional."[74]

Guideline 01/2022 clarifies that the objectives of data subjects in exercising DSAR must not play a role in assessing the validity of the request.[75] Daniel Cooper & Lars Lensdorf pointed out that this is one of the most controversial statements by EDPB as assessing the intent or objectives of the request are necessary to prevent abusive requests.[76] The purpose of DSAR is to "enable the data subject to ascertain and verify the lawfulness of the processing, and if necessary, to exercise their rights"[77] while other purposes, such as circumventing administrative procedures to gain access to documents or obtaining evidence for court proceedings should not be entertained by way of DSAR. Therefore, assessing the intent of hackers may not easily be possible under the EU GDPR and Indonesian PDP Law.

In addition to the sheer volume of DSAR, some companies may opt to immediately comply with any requests in fear of missing the timeline or choose not to refuse at all since the basis of DSAR refusal is ultimately vague. From that perspective, data controllers are more likely to comply with potentially invalid or fake DSAR.[78] Unlike other social engineering attempts, hackers can hide behind the legitimacy of DSAR to manipulate data controllers in justifying their access to data.[79] For instance, by sending vague DSAR requests and providing falsified documents, hackers could mislead data controllers to disclose personal data of affected data subjects.

---

[74] James Pavur and Casey Knerr, "GDPArrrrr: Using Privacy Laws to Steal Identities," *Blackhat USA 2019 Whitepaper* (December 2019): 4, https://doi.org/10.48550/arXiv.1912.00731.

[75] European Data, "Guideline 01/2022,"13.

[76] Daniel Cooper & Lars Lensdorf, "EDPB Draft Guidelines 01/2022 on Data Subject Rights – Right of Access", *Computer Law Review international* (March 2022): 57.

[77] EU General Data Protection Regulation, Recital 63.

[78] Pavur and Knerr, "GDPARRRR: Using Privacy," 2.

[79] Pavur and Knerr, "GDPARRRR: Using Privacy," 8.

In 2022, high-level data breaches in Indonesia exposed voluminous personal data and/or documents such as national IDs (KTP), tax numbers (NPWP), and official passports often used as DSAR's authentication measures.[80] Coupled with the non-existent verification guideline for handling DSAR, a scenario where hackers would have easily impersonated data subjects and abuse DSAR are very likely to occur. In January 2023, a criminal impersonated a bank customer using forged and stolen documents. This is a stark reminder on the verification procedural flaws in Indonesia.[81] With the opportunity to digitally impersonate customers, Rights to Access may become the next weapon for hackers to exploit. Within the Indonesian context, DSAR obligation applies to almost every business sector, ranging from sophisticated digital industry to small medium enterprises that operate traditionally with varied resource strength and bandwidth.[82] A "one-size fit all" approach in determining the time limit might not have been an ideal choice as it can burden business actors disproportionately.

III.A.3. Calibration, Recalibration, and Redaction

After authenticating the request, it is important to clarify the scope of request, and make sure that the requested information falls into the category of personal data that can be accessed under DSAR. Data controllers are encouraged not only to search within its online database, but also offline documents.[83] Calibrating the search criteria is also recommended by EDPB Guidelines 01/2022. For instance, if the requestor's personal data is stored in each category (name, date of birth, gender, and others) then the use of search criteria are in these structured data. However, data controllers have the discretion in determining how the search is conducted as long as it provides the accurate dataset.[84]

Throughout the search process, data controllers may discover the data compiled might have been mixed with non-personal data or third party's personal data. At this stage, the data controller must review, validate, redact, and repeat the exercise for quality assurance purposes. DSAR scope is not

[80] Izzat Ats Tsaqofi, "Kebocoran Data PeduliLindungi Valid? Begini Jawaban Pakar," *Voi.id*, November 17, 2022, https://voi.id/teknologi/228258/kebocoran-data-pedulilindungi-valid-begini-jawaban-pakar.

[81] Praditya Fauzi Rahman, "Pemilik Rp 320 Juta yang Dibobol Tukang Becak Pertanyakan Tanggung Jawab Bank," *DetikJatim,* January 23, 2023, https://www.detik.com/jatim/hukum-dan-kriminal/d-6529276/pemilik-rp-320-juta-yang-dibobol-tukang-becak-pertanyakan-tanggung-jawab-bank.

[82] Titah Arum M. R. Toewoeh, "Kominfo dan Kadin Sosialisasi UU PDP ke Pelaku Usaha," *Kominfo,* October 29, 2022, https://aptika.kominfo.go.id/2022/10/kominfo-dan-kadin-sosialisasi-uu-pdp-ke-pelaku-usaha/.

[83] European Data, "Guideline 01/2022," 123.

[84] Davinia Brennan, "The New Guidelines on Access Request – is the bar now too high?" *Data Protection Ireland,* vol. 15 (May 2022): 2.

the document in its entirety, but the data subject's personal data. Therefore, data controllers are mandated to disclose parts of document which contains personal data relating to the data subject's request and does not disclose other documents, information and third party's personal data.[85]

III.A.4 DSAR Exemption Check

Similar to another exercises of rights, there are limitations on how data subjects can utilise their Right to Access through DSAR. We limit our discussion on DSAR-specific exemptions and do not discuss the blanket exemptions on all data subject rights as set out in Article 23 of the EU GDPR restrictions. From the EU perspective, there are two grounds where data controllers can refuse to manage DSAR. First, Article 12 (5) stipulates "*[w]here request from a data subject are manifestly unfounded or excessive, in particular because of their repetitive characters, the controller may either (a) charge a reasonable fee … (b) refuse to act on the request.*"[86] Second, whether answering DSAR would balance the rights and freedoms of others as stipulated under Article 15 (4), data controllers must act cautiously before deciding to refuse to act on DSAR as the threshold of manifestly unfounded or excessive request is very high, and the data controller must also inform the requestor that DSAR has been rejected. For instance, a case where the court held that a DSAR was "manifestly unfounded" arises where a data subject is requesting documents utilised as evidence for civil litigation – in essence, DSAR was utilised as a *subpoena* and not as the intended purpose of verifying data processing.[87] However, data controllers are still obliged to inform the requestor if the request cannot be processed any further and direct it to supervisory authority for any future complaint.

Furthermore, EDPB Guideline 01/2022 provides the mechanisms for checking the limitations and restrictions of DSAR. In the case that the DSAR fulfilment would lead to negatively affecting the freedom of others (for instance, a financial report of a data subject also contains personal data of other persons such as sellers, management, or the counterpart of transactions), data controllers must check if such issue can be resolved by redacting the data as mentioned in the previous section before considering rejecting the request. In addition, it must also be noted that the scope of the Right to Access only extends to personal data and does not provide access to the related document in its entirety.

---

[85] Paul Buckle, "Data subject access requests and beneficiaries' rights to information," *Trusts & Trustees,* Vol. 25, No. 3, (April 2019): 336.

[86] EU General Data Protection Regulation, Article 12(5).

[87] Agencia Espanola Proteccion Datos, E/00739/2021.

Under the Indonesian PDP Law, data controllers may choose blanket exception against data subject rights under Article 15 or specific grounds to refuse DSAR under Article 33. Pursuant to Article 15, the Rights of Data Subject may be excluded for 1) In the interest of national defence and security; 2) Interest of law enforcement process; 3) Public interest in the context of state administration; 4) Interest of financial services, monetary, payment system, and financial system stability; and/or 5) Statistics and scientific research.[88] The mechanisms and specifications of this exception will be regulated in the implementing regulations.[89]

However, "in the interest of national defence and security" as exemption against data subject rights was challenged in the Indonesian Constitutional Court in April 2023. Appellant argued that the term can be interpreted too broadly and defeats the protection of data subject. The court rejected this argument, recognising the nature of such exemption is too broad to ensure that public interest can be protected as long as this exemption is done within the "prevailing laws and regulations."[90] Alternatively, data controller may opt to the refusal basis under Article 33 in the event that it 1) endangers the security, physical health, or mental health of data subject or other people; 2) discloses third party personal data; and 3) contrary to the interests of national defence and security.[91] However, it has not been clarified on the scope and how can data controller articulate this basis to reject DSAR. Therefore, it is imperative to set out detailed specifics on the grounds where DSAR can be rejected similar to the EU GDPR and EDPB Guidelines 01/2022.

III.A.5. DSAR Secure Delivery

As the final step of DSAR, data controllers must deliver copies of requested personal data over a secured platform to data subjects. Data controllers might need to consider if specific assistances or requirements is needed (if a data subject is unable due to physical condition or being represented by a guardian or trusted person). In practice, secure delivery is done by way of secured 'https' links that can be accessed by data controller and data subject only. If the request is represented by an authorised person, for example, a solicitor or a barrister, the authorised person will get access to the link and be able to download and confirm relevant scanned documents or batch of scanned documents that resonate the request. However, certain data controllers might not be able to set up appropriate technical configurations due to lack of DSAR

[88] Indonesia, Law No. 27 of 2022, Personal Data Protection Act, Article 15 (1).
[89] Indonesia, Law No. 27 of 2022, Personal Data Protection Act, Article 15 (2).
[90] Indonesian Constitutional Court, Decision Number 110/PUU-XX/2022, pp. 100-102.
[91] Indonesia, Law No. 27 of 2022, Personal Data Protection Act, Article 33.

workflow awareness, tools, or platform that might accelerate the process. In this scenario, it is indispensable for data controllers to manage data subject's timeline expectation whilst fulfilling with such request. Appropriately, data controllers should reflect its commitment via internal DSAR policy and/or Data Protection Notice and Policy.

IV. CROSS-JURISDICTIONAL DSAR: THE CASE CONCERNING ASEAN QRIS PAYMENT SYSTEM REQUESTS

Among the most recent development in the Financial & Technology sector is the deployment of Quick Response Code Indonesian Standard ("QRIS"), which acts to standardize QR code for all payment providers – thus enabling interoperability between e-wallet and payment providers.[92] QRIS is regulated under Bank Indonesia Governor Board Member Regulation No. 21/18/2019 (last amended by PADG 24/1/2022) that governs the domestic and cross-border use of QRIS.[93]

The programme was first launched in 2019 to accelerate financial inclusion and digital payment accessibility for Micro Small Medium Enterprise (MSMEs) in Indonesia, but now QRIS model is also utilised to facilitate cross border QR Payment Linkages as agreed on by various Government-to-Government arrangements.[94] During its Indonesia G20 Presidency, five central banks of major ASEAN countries (Bank Indonesia, Bank Negara Malaysia, Bank of Thailand, Bangkok Sentral ng Pilipinas, and Monetary Authority of Singapore) signed the Memorandum of Understanding on Cooperation in Regional Payment Connectivity to facilitate cross-border QR Codes and Fast Payments by 2025.[95] While from the economic perspective, this will accelerate growth in the region, the personal data processing activities within this technology should be addressed appropriately.

The QR Code initiative involves multiple data controllers, data processors or joint data controllers and processors from private entities. For instance, in the pilot project between Bank of Indonesia and Bank of Thailand, 76 financial

---

[92] Oxford Analytica, "Fintech growth outpaces regulation in Indonesia", *Expert Briefings*, accessed on 18 February 2023] https://doi.org/10.1108/OXAN-DB264128.

[93] Bank Indonesia, Governor Board Member Regulation No. 21/18/PADG/2019 on the Implementation of QRIS Standard for Payment, Article 18.

[94] Perry Warjiyo and Solikin M. Juhro, Central Bank Policy Mix: Key Concepts and Indonesia's Experience dalam Central Bank Policy Mix: Issues, Challenges, and Policy Responses, (Jakarta: BI Institutes, 2022), 15.

[95] Communication Department of Bank Indonesia, "Central Banks of Indonesia, Malaysia, Philippines, Singapore and Thailand Seal Cooperation in Regional Payment Connectivity," Bank Indonesia, November 14, 2022, https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_2430822.aspx.

service providers are involved in assisting cross-border QR code transactions from customers to merchant.[96] Eventually, the financial service providers and related Fintech companies will process personal data of consumers throughout the ASEAN region.

An Indonesian tourist can conduct transaction through QR code at Chatuchak Market in Thailand, at which the Thailand's Fintech company will have financial records that contain personal data of the Indonesian tourist. In this scenario, the tourist, as data subject will be able to send out DSAR to these Fintech companies. While we have highlighted the problems of handling domestic DSAR, a Cross-Border DSAR would create another layer of complexity due to different timeline below:

Table 3. Comparative DSAR Timeline

Country	DSAR Timeline
Indonesia	3 x 24 Hours (Non-Extendable)
Malaysia	21 Days (Extendable)
Thailand	30 Days (Non-Extendable)
Philippines	Subject to nature and complexity of DSAR
Singapore	30 Days (Extendable)

As illustrated above, different timelines might pose burdensome to Fintech companies as they would eventually need to comply with country specific DSAR timeline. This also fails to consider that every country shall have different verification mechanisms considered "proportionate" as part of authenticating request before disclosing any data (including financial transactions data). A harmonisation effort akin to the EU, bearing in mind the interconnectedness of ASEAN digital economy might be an interoperable solution.

This issue does not only arise on QR-based cross border payment system, but also occurs in all aspects of Fintech DSAR in the ASEAN region. In February and March of 2023, we conducted a privacy policies and notices analysis of leading and reputable Fintech companies in Indonesia, Singapore, Philippine, and Malaysia while comparing it to matured data protection law from the UK and the EU. From this analysis, we learnt three crucial points: 1) In developing countries like Indonesia, there is generic information relating to DSAR; 2) Several Fintech companies have yet to specify a designated DPO as main DSAR point of contact whether by manual or direct communications; and 3) Language barriers shall become an issue in cross-jurisdictional DSAR as most privacy policies and notices are written in local language, instead

[96] Communication Department of Bank Indonesia, "Indonesia dan Thailand Meresmikan Implementasi Pembayaran Kode QR Lintas Negara," Bank Indonesia, August 29, 2022, https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2423222.aspx.

of bilingual or multilingual (for instance, privacy policies and notice of an Indonesian Fintech company is only available in Bahasa Indonesia, but not other languages) which renders data subject outside Indonesia struggles to understand how their personal data is being processed and importantly to effectuate future DSAR.

In 2016, ASEAN adopted the Framework on Personal Data Protection, among other things, recognising the Rights to Access as part of the principles of personal data protection in the region.[97] However, the principle mentions that the access should be provided "within a reasonable period of time" and ASEAN member states have different DSAR timeline and requirements despite this framework. Therefore, we propose two approaches. First, to create a uniform timeline and cross-border DSAR requirements across the region or at least between member states that have signed the Memorandum of Understanding on Cooperation in Regional Payment Connectivity. Second, to provide a clear exemption that can be used, when necessary, by Fintech companies in the QR-Code or international payment systems in the region. To deep dive into these, and to avoid prospective ambiguity, we commendably suggest ASEAN member states to consider the two approaches as part of future consultation, to be coordinated and aligned with respective member states' data protection regulators, central banks, and other sector specific regulators.

IV. CONCLUDING REMARKS

To conclude, we have established the fundamentals of DSAR for data subjects and data controllers. As a developing country, there will be practical challenges relating to DSAR implementation in Indonesia, mainly derived from undeveloped implementing guidelines and lack of awareness on the exercise of data subject rights. In this article, we have provided the historical background of Indonesia PDP Law, influenced deeply by the EU GDPR, and showcased how DSAR is being practiced in developed countries. Visually, we illustrated DSAR workflow that might be useful to be considered in forthcoming DSAR implementing regulations in Indonesia, aimed at avoiding legal uncertainty and contextualized baseline global best practice. The implication of this paper highlighted the current DSAR framework under Indonesian law is technically challenging to operationalise since many aspects remained missing.

[97] "Framework On Personal Data Protection," ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), accessed on 20 February 2023. https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

We admit that Indonesian PDP Law implementing regulation is still in drafting phase and recognise the sophisticated cross-border payments and rapid growth of Fintech technologies in ASEAN. We intertwined Fintech's data processing activities and DSAR that could pose practical compliance challenge domestically, regionally, and internationally. From an eagle's eye view, diverging global DSAR timeline and requirements might trigger excessive compliance cost for Fintech companies and non-Fintech companies that process voluminous dataset (Indonesian, ASEAN, and non-ASEAN personal data, including but not limited to the EU dataset). As an interoperable solution, we proposed a common framework that harmonise DSAR management, and unboxed the strict, but arbitrary DSAR timeline set forth in several jurisdictions in ASEAN member states, including Indonesia. Moving forward, we will continue to volunteer, engage, and be part of future stakeholders' consultation to shape Indonesia and ASEAN DSAR harmonisation in 2024 and beyond.

REFERENCES

Abubakar, Lastuti and Tri Handayani. "Financial Technology: Legal Challenges for Indonesia Financial Sector." *IOP Conf. Series: Earth and Environmental Science* 175, (2018): 3.

Algamar, Muhammad Deckri and Noriswadi Ismail. DSAR Awareness Question Survey Results. 2023.

Agusta, Hendrawan. "Keamanan dan Akses Data Pribadi Penerima Pinjaman dalam Peer to Peer Lending di Indonesia," *KRTHA Bhayangkara*, no. 1 (June 2021): 18-19. https://doi.org/10.31599/krtha.v15i1.289.

Agustini, Pratiwi. "UU PDP Akan Permudah Pertukaran Data dengan Negara Lain." *Direktorat Jenderal Aplikasi Informatika."* Accessed January 21, 2023. https://aptika.kominfo.go.id/2020/11/uu-pdp-akan-permudah-pertukaran-data-dengan-negara-lain/.

Ausloos, Jef, and Pierre Dewitte. "Shattering One-Way Mirrors. Data Subject Access Rights in Practice." *International Data Privacy Law* 8, (2018): 30.

Alekseenko, Aleksandr P. *Global Perspectives in FinTech: Law, Finance and Technology.* London: Palgrave Macmillan, 2022

Asean Telecommunications and Information Technology Ministers Meeting. "Framework On Personal Data Protection." Accessed on [DATE], https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

Bambauer, Derek E. "Privacy Versus Security." *Journal of Criminal Law and Criminology* vol. 103 (Summer 2013): 679.

Banisar, David. "Privacy & Human Rights an International Survey of Privacy Laws and Developments." *The John Marshall Journal of Computer & Information Technology,* vol. XVIII (January 1999): 6.

Boot, Arnoud, Peter Hoffmann, Luc Laevenc, Lev Ratnovski. "Fintech: what's old, what's new?" *Journal of Financial Stability* 53, (2021). *https://doi.org/ 10.1016/j.jfs.2020.100836*

Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review*, no. 1 (2015): 1–68.

Brennan, Davinia. "The New Guidelines on Access Request – is the bar now too high?" *Data Protection Ireland,* vol. 15 (May 2022): 2.

Buckle, Paul. "Data subject access requests and beneficiaries' rights to information." *Trusts & Trustees*, Vol. 25, No. 3, (April 2019): 336.

Budhijanto, Danrivanto, "Cybersecurity dan Hukum Pelindungan Data Pribadi di Indonesia," in *Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity*. Bandung: Refika Aditama, 2023.

Chivot, Eline and Daniel Castro. "The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy." *Centre for Data Innovation.* May 13, 2019. https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/.

Cluley, Graham. "1&1 Telecom GmbH hit by almost €10 million GDPR fine over poor security at call centre." *Security Boulevard,* last modified December 11, 2019. https://securityboulevard.com/2019/12/11-telecom-gmbh-hit-by-almost-10-million-gdpr-fine-over-poor-security-atcall-centre.

Communication Department of Bank Indonesia. "Indonesia dan Thailand Meresmikan Implementasi Pembayaran Kode QR Lintas Negara." Bank Indonesia, August 29, 2022. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2423222.aspx.

Data Protection Commission. "Irish Data Protection Commission's Annual Report 2021." *An Coimisiun Chosaint Sonrai,* February 24, 2022, 30.

Degerli, Kazim. "Regulatory Challenges and Solutions for Fintech in Turkey." *Procedia Computer Science* 158 (2019)*:* 935.

Dewi, Sinta. "Balancing Privacy Rights and Legal Enforcement: Indonesia Practices."

Esteves, Beatriz, Vıctor Rodriguez-Doncel, and Ricardo Longares. "Automating the Response to GDPR's Right of Access." *Legal Knowledge and Information Systems* (2022): 171. https://doi.org/10.3233/FAIA220462

Fintech Indonesia. "Masukan dan Pandangan Industri Fintech atas Rancangan Undang-Undang Perlindungan Data Pribadi." Accessed on 12 January 2023 https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200706-021940-3243.pdf.

Fintech Indonesia. "Rancangan Undang-Undang Data Pribadi." Accessed on 12 January 2023, https://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200706-022052-5497.pdf.

Fortuna, Gabriella Zanfir. The EU General Data Protection Regulation (GDPR): A Commentary: 4553.

Gai, Keke, Meikang Qui, Xiaotong Sun. "A survey on FinTech." *Journal of Network and Computer Applications*, vol. 103 (2018): 262–273.

Galetta, Antonella, Paul de Hart, Xavier L'Hoiry, Clive Norris. "Mapping the Legal and Administrative Frameworks of Access Rights in Europe: A Cross-European Comparative Analysis." Work Package 5 for the IRISS Project (2014).

Greenleaf, Graham. "Data Privacy Laws in Asia: Context and History." In *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, 9–10. United Kingdom: Oxford University Press, 2017.

Hernández, Elena, Mehmet Öztürk, Inés Sittón & Sara Rodríguez. "Data Protection on Fintech Platforms." *International Conference on Practical Applications of Agents and Multi-Agent Systems*, vol. 1047 (June 2019): 223–233. https://doi.org/10.1007/978-3-030-24299-2_19.

International Association of Privacy Professionals and Ernst & Young. "IAPP-EY Annual Privacy Governance Report 2018." Accessed January 21, 2023. https://iapp.org/resources/article/iapp-ey-annualgovernance-report-2018/.

International Journal of Liability and Scientific Enquiry 5, (February 2012): 233. https://doi.org/10.1504/IJLSE.2012.051961.

Kameo, Jeferson. "Panama Papers dan Diskursus tentang Perlindungan Data di Indonesia: Suatu Perspektif Teori Keadilan Bermartabat." *Jurnal Refleksi Hukum,* no. 1, (2016): 92. https://doi.org/10.24246/jrh.2016.v10.i1.p84-98.

Kuchler, Hannah. "Max Schrems: the man who took on Facebook - and won." *The Irish Times,* April 5, 2018. https://www.irishtimes.com/business/technology/max-schrems-the-man-who-took-on-facebook-and-won-1.3451485.

Lauradoux, Cedric. Privacy Technologies and Policy 10th Annual Privacy Forum, APF 2022 Warsaw, Poland, June 23–24, 2022, Proceedings. Warsaw: APF 2022, 2022.

Lewis, Paul and Paul Hilder, "Leaked: Cambridge Analytica's blueprint for Trump victory," The Guardian, March 23, 2018. https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trumpvictory/

Linden, Thomas, Rishabh Khandelwal, Hamza Harkous. "The Privacy Policy Landscape After the GDPR." *Proceedings on Privacy Enhancing Technologies,* no. 1 (2020): 48-49. https://doi.org/10.2478/popets-2020-0004.

Lloyd, Ian J. *Information Technology Law*. United Kingdom: Oxford University Press, 2014.

Makarim, Edmon. *Pengantar Hukum Telematika*. Depok: PT Raja Grafindo Persada, 2005.

Martino, Mariano Di, Pieter Robyns, Winnie Weyts , Peter Quax. "Personal Information Leakage by Abusing the GDPR "Right of Access." *Fifteenth Symposium on Usable Privacy and Security,* (August 2019): 374.

Moore, Jina. "Cambridge Analytica Had a Role in Kenya Election, too." The New York Times, March 20, 2018. https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html/

Nissenbaum, Helen. Privacy In Context: Technology, Policy, And the Integrity of Social Life. California: Stanford University Press, 2010.

Olavia, Lona. "Industri Minta Kepastian Hukum Perlindungan Data Pribadi." *BeritaSatu.com,* March 30, 2021. https://www.beritasatu.com/ekonomi/753123/industri-minta-kepastian-hukum-perlindungan-data-pribadi.

Pavur, James and Casey Knerr. "GDPArrrrr: Using Privacy Laws to Steal Identities." *Blackhat USA 2019 Whitepaper* (December 2019): 4. https://doi.org/10.48550/arXiv.1912.00731.

Peers, Steve, Tamara Harvey, Jeff Kenner, Angela Ward. *The EU Charter of Fundamental Rights: A Commentary*. Oxford: Hart Publishing, 2014.

Petrova, Anastasia. "The Impact of the GDPR Outside the EU." *Lexology.com*, September 17, 2019. https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f.

Peukert, Christian, Stefan Bechtold, Tobias Kretschmer, and Michail Batikas. "Regulatory export and spillovers: How GDPR affects global markets for data." *Centre for Economic Policy Research*. September 30, 2020. https://cepr.org/voxeu/columns/regulatory-export-and-spillovers-how-gdpr-affects-global-markets-data.

Power, Ed . "The Great Hack: The story of Cambridge Analytica, Trump and Brexit." The Irish Times, July 24, 2019. https://www.irishtimes.com/culture/tv-radio-web/the-great-hack-the-story-of-cambridge-analytica-trump-and-brexit-1.3965788.

Pratomo, Yudha. "Google Sebut UU Perlindungan Data Pribadi Bisa Menyusahkan Startup." *Kompas.com*, August 28, 2019. https://tekno.kompas.com/read/2019/08/20/14050087/google-sebut-uu-perlindungan-data-pribadi-bisa-menyusahkan-startup?page=all.

Presthus, Wanda and Kaja Felix Sønslien. "An analysis of violations and sanctions following the GDPR." *International Journal of Information Systems and Project Management*, no. 1 (2021): 45-46. https://doi.org/10.12821/ijispm090102.

Rahman, Praditya Fauzi. "Pemilik Rp 320 Juta yang Dibobol Tukang Becak Pertanyakan Tanggung Jawab Bank." *DetikJatim,* January 23, 2023. https://www.detik.com/jatim/hukum-dan-kriminal/d-6529276/pemilik-rp-320-juta-yang-dibobol-tukang-becak-pertanyakan-tanggung-jawab-bank.

Rosadi, Sinta Dewi, Siti Yuniarti, and Rizki Fauzi. "Protection of Data Privacy in the Era of Artificial Intelligence in the Financial Sector of Indonesia." *Journal of Central Banking Law and Institutions,* no. 2, (2022): 353-366. https://doi.org/10.21098/jcli.v1i2.18.

Shafira, Dini Ima. "DPR Resmi Sahkan RUU Perlindungan Data Pribadi." *Tempo.co*, September 20, 2022. https://nasional.tempo.co/read/1636301/dpr-resmi-sahkan-ruu-perlindungan-data-pribadi.

Smedinghoff, Thomas J. "The Duty to Verify Identity: A Critical Component of Privacy and Security Compliance." *PLI 22nd Annual Institute on Privacy & Cybersecurity* (April 2021): 10.

Soelistyo, Andre. "UU PDP & Kepatuhan Industri." *Bisnisindonesia.id*, October 6, 2022.

Solove, Daniel J. *The Digital Person, Technology, and Privacy in the Information Age*. New York: New York University Press, 2004.

Sugiyanti, Umi and Agung Pambudi. "Perlindungan Data Privasi dan Kebebasan Informasi dalam Platform WhatsApp." *Jurnal Ikatan Pustakawan Indonesia*, no. 2 (2022): 67.

Tang, Alan. "Data Subject Rights, Inquiries, and Complaints" in *Privacy in Practice: Establish and Operationalize a Holistic Data Privacy Programme*, 398. Abingdon: CRC Press, 2023.

Toewoeh, Titah Arum M. R. "Kominfo dan Kadin Sosialisasi UU PDP ke Pelaku Usaha." *Kominfo,* October 29, 2022. https://aptika.kominfo.go.id/2022/10/kominfo-dan-kadin-sosialisasi-uu-pdp-ke-pelaku-usaha/.

Tsaqofi, Izzat Ats. "Kebocoran Data PeduliLindungi Valid? Begini Jawaban Pakar." *Voi.id*, November 17, 2022. https://voi.id/teknologi/228258/kebocoran-data-pedulilindungi-valid-begini-jawaban-pakar.

Vrabec, Helena. *Data Subject Rights under the GDPR with a Commentary Through the Lens of Data-Driven Economy*. New York: Oxford University Press, 2021.

Warren, Samuel and Louis Brandeis. "The Right to Privacy." *Harvard Law Review*, no. 5 (December 1890): 193-220.

REGULATIONS

Agencia Espanola Proteccion Datos, E/00739/2021.

European Union, Regulation 2016/679 General Data Protection Regulation

European Commission, Directive 95/46/EC Data Protection Directive

European Data Protection Board. Guidelines 01/2022 on data subject rights - Right of access.

Indonesia. Law No. 23 of 2006 on Citizen Administration, Article 79 (Amended by Law No. 24 Year 2003).
Indonesia. Law No. 27 of 2022 on Personal Data Protection.
Indonesia. Bank Indonesia Regulation No. 19/12/PBI/2017 on Financial Technology Implementation.
Indonesia. Bank Indonesia Regulation No. 23/15/PBI/2021 on Central Bank Services
Indonesia. Bank Indonesia Board Member Regulation No. 21/18/PADG/2019 on QRIS Standard Implementation for Payment
Indonesia. Financial Service Authority Regulation No. No. 23/POJK,01/2019 on AML & Money Laundering Prevention
Singapore. Personal Data Protection Commission Singapore.
United States. The California Consumer Privacy Act of 2018.

This page is intentionally left blank