Lex Scientia Law Review

ISSN 2598-9677 (Print)
ISSN 2598-9685 (Online)
VOLUME 5 ISSUE 2, NOVEMBER 2021
DOI: 10.15294/lesrev.v5i2.50601

TYPE: RESEARCH

Analysis Principles of Personal Data Protection on COVID-19 Digital Contact Tracing Application: PeduliLindungi Case Study

Anugrah Muhtarom Pratama
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
Email: pratamaanugrah23@gmail.com
ORCID Link: https://orcid.org/0000-0003-3814-0239

Umi Khaerah Pati
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia

Citation:
Pratama, A. M. & Pati, U. K. (2021). Analysis Principles of Personal Data Protection on COVID-19 Digital Contact Tracing Application: PeduliLindungi Case Study, Lex Scientia Law Review, 5(2), 65-88, doi: https://doi.org/10.15294/lesrev.v5i2.50601.

History of Article
Received: October 05, 2021
Revised: November 11, 2021
Accepted: November 19, 2021

Lex Scientia Law Review published by Faculty of Law, Universitas Negeri Semarang, Indonesia in collaboration of UKM Lex Scientia. Published biannually every May and November.

ABSTRACT

This article aims to review the application of the principle of personal data protection as part of privacy rights in the PeduliLindungi application considering that on the one hand, the PeduliLindungi application helps the government to reduce the spread of the COVID-19 virus. But on the other hand, there is a threat of misuse of personal data in the future. This background article is based on the use of the PeduliLindungi application, which was initially used to track the spread of the virus during the COVID-19 pandemic. But it seems that the public will increasingly use its use in the future, especially now that it has begun to be planned as an e-wallet and started integrating with several other applications. This article reveals that there has been a dual role by the Ministry of Communication and Informatics as a supervisor and controller of personal data in Indonesia so that it has implications for the PeduliLindungi application that has not fully applied the principles of personal data protection when collecting, processing, and storing personal data. For the future, a comprehensive legal development drive is needed related to the protection of personal data. There is a personal data protection agency and Data Protection Officer (DPO) to more strongly enforce the principles of personal data protection.

KEYWORDS
Digital Tracing Applications; Pedulilindungi; Principles; Protection Of Personal Data; Tracing

1. INTRODUCTION

The rapid development and application of technology have resulted in the increasingly easy flow of information obtained by the public in all aspects of life. The story of globalization, especially internet-supported technology, has colored the trade sector's growth from traditional trade, which then turned into e-commerce. The existence of e-commerce has allowed transactions to be made within countries and between countries that can create unlimited agreements between space and time. This development makes trade between countries faster, and in the end, the country's borders are not a significant problem.[1] Not to mention the growth of fintech that is increasingly growing until now.

The increasingly frequent phenomena of technological development make many people increasingly use technology in their daily lives and help facilitate and increase work productivity, build socio-economic relationships and make things easier. But it cannot deny that almost all activities in people's lives today require personal data. Given that personal data has become the new oil, it is indirectly necessary to properly manage and account for collecting, processing, and storing personal data.[2] Because according to James Adams and Richard Kletter, technology is interrupted every night, so technology is like a double-edged sword because, on the one hand, it offers a variety of conveniences, but on the other hand also brings crucial legal issues, including personal data.[3] Therefore, the public desperately needs personal data protection today to remain safe and reduce their concerns in using various types of technology.

This concern is essential to note because humans today have entered into significant data civilizations. The biggest problem faced in the era of big data is the security aspect of personal data.[4] Humans understand that

---

[1] Deky Paariadi, "Pengawasan E-Commerce dalam Undang-Undang Perdagangan dan Undang-Undang Perlindungan Konsumen", *Jurnal Hukum dan Pembangunan*, Volume 48 Number 3, 2018, p. 653.

[2] Larry Ozeran, Anthony Solomonides, and Richard Schreiber "Privacy versus Convenience: A Historical Perspective, Analysis of Risks, and an Informatics Call to Action", *Applied Clinic Informatics*, Volume 12 Number 2, 2021, p. 274.

[3] James Adams and Richard Kletter, *Artificial Intelligence: Confronting The Revolution*, Endeavour Media Ltd, California, 2018, p. 19.

[4] Danrivanto Budhijanto, *Cyber Law Dan Revolusi Industri 4.0*, Logoz Publishing, Bandung, 2019, p. 186.

DOI: 10.15294/lesrev.v5i2.50601

personal data has become an invaluable new oil these days. The value of personal data is understandable because, in today's reality, tracing, collecting, examining, and analyzing various information about people is the most crucial new connection of the big data civilization.[5] Moreover, today, many public bodies and companies are increasingly realizing the importance of big data as a strategic source because it can quickly identify trends and patterns of people's needs only through analyzing human behavior habits.[6]

Furthermore, personal data has also attracted the attention of many people, especially when personal data can currently be stored and transmitted on existing hardware, software, and networks for various purposes.[7] Not least, the application of big data on digital contact tracing applications during the COVID-19 pandemic is rated the largest and most ambitious use of personal data ever carried out by countries in the world to fight and reduce the spread of COVID-19.[8] The actual evidence is evident with almost all countries implementing the COVID-19 digital contact tracing application. (See Figure 1 in green).

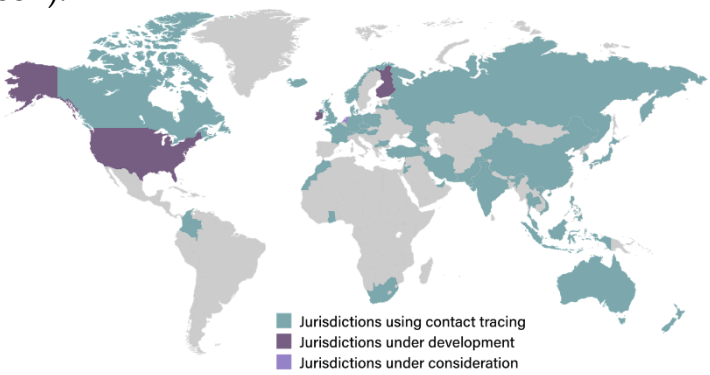

Figure 1. Countries Using the COVID-19 Digital Contact Tracing App.
Source: Norton Rose Fullbright

Nevertheless, the virtues of implementing big data using technology have presented legal risks, such as many highlights related to more accessible access to people's data in the use of the COVID-19 digital contact tracing application.[9] On the one hand, the use of the COVID-19 digital contact tracing

[5] Youssra Riahi, "Big Data and Big Data Analytics: Concept, Types, and Technology", *International Journal of Research and Engineering*, Volume 5 Number 9, 2015, p. 525.

[6] Noriko Higashizawa and Yuri Aihara, "Data Privacy Protection of Personal Information Versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)", *Defense Counsil Journal*, Volume 84 Number 1, 2017, p. 1.

[7] Julian Jang Jaccard, "A Survey of Emerging Threats in Cybersecurity", *Journal of Computer and System Sciences*, Volume 80 Numberr 5, 2014, p. 973.

[8] Robert A. Fahey dan Airo Hino, "COVID-19, Digital Privacy, and the Social Limits on Data-Focused Public Health Responses", *International Journal of Information Management*, Volume 55, 2020, p. 1.

[9] Mariarosaria Taddeo, "The Ethical Governance of the Digital During and After the COVID-19 Pandemic", *Minds and Machines*, Volume 30, 2020, p. 171.

DOI: 10.15294/lesrev.v5i2.50601

application helps the government because it can quickly find out the location of those who contracted the COVID-19 virus to facilitate tracing, those who are fine, those who do crowding activities, or those who do not travel and at home only.[10] With the existence of this data, the government can see the level of the affected communities and, at the same time, formulate control policies such as community restrictions. Furthermore, the utilization of big data in the COVID-19 digital contact tracing application is part of implementing a smart city that realizes the integration of stakeholders in maintaining and protecting the public from the threat of exposure to the COVID-19 virus.[11]

In preventing the misuse of personal data, each country must implement the principles of personal data protection based on the law to ensure the security and safety of COVID-19 digital tracing applications.[12] In Indonesia, through the Decree of the Minister of Communication and Informatics No. 171 of 2020 on the Determination of Pedulilindungi Application in the Framework of Health Surveillance handling Corona Virus Disease 2019 (COVID-19), COVID-19 digital contact tracing application is issued PeduliLindungi. Kominfo developed the PeduliLindungi application with the support of PT. Telkom Indonesia Tbk aims to assist the government in tracing to stop the spread of the COVID-19 virus.

Through this application, it is expected that control of the spread of the COVID-19 virus could be monitored and, most importantly, detect as early as possible people who are positive for COVID-19 for the next step of handling. Interestingly, the phenomenon of COVID-19 digital contact applications is currently used for tracing and has begun to switch to use as electronic vaccine certificate storage. Even in Indonesia, the PeduliLindungi application is being planned to be used as an e-wallet and integrated with 11 applications. Regardless of what is offered, it becomes an important question to answer as to whether the PeduliLindungi application has implemented the principles of personal data protection or vice versa. To that end, this article will explore the application of personal data protection principles in the PeduliLindungi application.

So far, there have been several discussions regarding the analysis of personal data protection related to the use of PeduliLindungi application, such as Denindah Olivia et al. (2020), which compares the use of PeduLindungi with Australia's Covidsafe. His research concluded that

---

[10] Ibid, 173.

[11] Pujiyono, Kukuh Tejomurti, Pranoto, dan Umi Khaerah Pati "The Principle of Proportionality in Using Smart City Cloud Computing For Patients Privacy Rights Protection in Handling the Covid-19 Pandemic", *Solid State Technology*, Volume 63 Number 4, 2020, p. 1122.

[12] Agung Kurniawan Sihombing and Yogi Bratajaya, "Contact Tracing Apps in Asean : A Threat to Privacy and Personal Data", *Kathmandu School of Law Review*, Volume 8 Number 1, 2020, p. 53.

DOI: 10.15294/lesrev.v5i2.50601

Indonesia could adopt regulations such as in Australia regarding the provision of criminal sanctions in fines for data controllers if found to violate personal data protection regulations.[13] Then Tiara Almira Raila et al. (2020) concluded the same thing as the previous writing, only to compare it with Singapore.[14] Next is Nurhidayanti et al. (2020), who discusses the protection of personal data on the PeduliLindungi application based on Permenkominfo, Health Law, Population Administration Law.[15]

Of the several articles that have been there, no party has analyzed more deeply related to the issue of applying personal data protection principles to the PeduliLindungi application. Analysis of this principle becomes vital to know whether the PeduliLindungi application has been appropriate in applying the principles of personal data protection or still ignores it. With the fulfillment of the principle of personal data protection, the security of personal data protection in the PeduliLindungi application can be more created. Conversely, if the PeduliLindungi application has not fully applied the principles of personal data protection, it can potentially misuse personal data in the future.

The structure of the article after Part 1 of this introduction will be divided into several parts. Part 2 will discuss the methods used. Part 3 is a discussion that is divided into two. Discussion in part A will review the application of personal data protection principles based on the European Union General Data Protection Regulation (EU GDPR) regime considering that Indonesia does not yet have a comprehensive personal data protection law framework and the selection of EU GDPR because in the Personal Data Protection Bill (PDP Draft) that is being drafted currently using the same principles as the EU GDPR.[16] In part B, will focus on developing personal data protection laws in Indonesia in the future by focusing on the existence of a personal data protection agency and Data Protection Officer (DPO). Part 4 is the last part of the cover that contains conclusions and suggestions.

---

[13] Denindah Olivia, Sinta Dewi Rosadi, dan Rika Ratna Permata "Perlindungan Data Pribadi Dalam Penyelenggaraan Aplikasi Surveilans Kesehatan Pedulilindungi Dan Covidsafe Di Indonesia Dan Australia", *Datin Law Journal*, Volume 1 Number 2, 2020, p. 14.

[14] Tiara Almira Raila, Sinta Dewi Rosadi, dan Rika Ratna Permata "Perlindungan Data Privasi Di Indonesia Dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan COVID-19 Dan Tanggungjawabnya", *Jurnal Kepastian Hukum Dan Keadilan*, Volume 2 Number 1, 2020, p. 14.

[15] Nurhidayati, Sugiyah, dan Kartika Yuliantari "Pengaturan Perlindungan Data Pribadi Dalam Penggunaan Aplikasi PeduliLindungi", *Widya Cipta: Jurnal Sekretari Dan Manajemen* Volume 5 Number 1, 2021, p. 44.

[16] See in the Principles of Drafting Personal Data Protection Norms in the Academic Text of the Personal Data Protection Bill 2020.

DOI: 10.15294/lesrev.v5i2.50601

2. METHOD

This writing uses a type of normative legal research, which is a procedure and a way of scientific research to find the truth based on the logic of legal science in terms of normative through the study of literature.[17] The types of approaches the Authors use are the statutory approach, comparative approach, and conceptual approach.

3. RESULT AND DISCUSSION

A. Analysis Principle of Personal Data Protection on PeduliLindungi Applications

The health world has long known tracing as a powerful way to overcome a prevention and disease problem. Tracing is done by monitoring the state of the community, then collecting the data obtained, and analyzing it to be used as data that is often known as surveillance. The development, currently with the use of technology, tracing has traditionally changed with digital surveillance.[18] As is now faced by all countries worldwide, namely COVID-19, digital surveillance has played an important role by using technology to widely track the spread of the COVID-19 virus through digital contact tracing applications.[19] Widely today has made many countries have developed the digital contact tracing application COVID-19, which is undeniable its existence presents the challenge of privacy protection in the form of personal data.[20]

In Indonesia, the COVID-19 digital contact tracing application used is PeduliLindungi. The PeduliLindungi application is the first moment for tracing to trace the connections of COVID-19 sufferers. Then it is perfected to store electronic vaccine certificates and has become a prerequisite for public activities and mobility through transportation. But now, the PeduliLindungi application began to be planned and widened to be used as an e-wallet and integrated into several applications. There is a more significant concern in the

---

[17] Johnny Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif, Bayu Media Publikasi, Malang, 2006, p. 57.

[18] Natalie Ram and David Gray, "Mass Surveillance in the Age of COVID-19", *Journal of Law and the Biosciences*, Volume 7 Number 1, 2020, p. 17.

[19] M. Thangavel & P. Varalakshmi B. Sowmiya, V.S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, "A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19", *SN Computer Science*, Volume 2 Number 136, 2021, p. 4.

[20] Rahman Molla Rashied Hussein, Abdullah Bin Shams, Ehsanul Hoque Apu, Khondaker Abdullah Al Mamun, dan Mohammad Shahriar "Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations", in *2nd International Conference on Advanced Information and Communication Technology*, IEEE, 2020, p. 1–2.

DOI: 10.15294/lesrev.v5i2.50601

development because there is the potential for misuse of personal data if many people have downloaded it.

It becomes increasingly worrying to see the principles of personal data protection in Indonesia today still weak. Shinta Dewi Rosadi as a personal data law expert Universitas Padjadjaran said that personal data protection regulations in Indonesia are still prevalent, so they cannot apply the principles of personal data protection.[21] But the good news, currently in Indonesia is drafting a PDP Draft that leans into EU GDPR, including the use of personal data protection principles. As is known, the EU GDPR personal data protection regulation is the most comprehensive regulation until now mainly because it has seven principles that have been the key to ensuring the protection of personal data for each data subject.[22]

Because Indonesia has not passed the PDP Draft, the Authors, in analyzing the PeduliLindungi application, will compare the principles of personal data protection belonging to the EU GDPR. Comparative does not matter because Indonesia is currently preparing the PDP Draft using the EU GDPR reference. In addition to the reasons for similarities, the EU GDPR has been believed to have exemplary implementation compared to personal data protection regulations in other countries.[23] One of them is seen with South Korea, which has asked for the European Data Protection Board (EPDB) in the preparation of personal data protection to be adequate for the country.[24] Therefore, the Author will analyze personal data protection principles in the PeduliLindungi application based on the EU GDPR. The principles of protection of EU GDPR personal data under Article 5 include:

1) Prinsip Keabsahan, Keadilan, dan Transparansi

[21] Sinta Dewi Rosadi, "Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi", *Arena Hukum*, Volume 9 Number 3, 2016, p. 418.

[22] Michelle Goddard, "The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact", *International Journal of Market Research*, Volume 59 Number 6, 2017, p. 703.

[23] Rachel L. Trotogott, "A Comparative Analysis of Data Privacy Impacted by Covid-19 Contact Tracing in the European Union, the United States, and Israel: Sacrificing Civil Liberties for a Public Health Emergency", *ILSA Journal of International & Comparative Law*, Volume 27 Number 1, 2020, p. 70.

[24] European Data Protection Board, "Opinion 32/2021 Regarding the European Commission Draft Implementing Decision according to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the Republic of Korea," 28 September 2021, accessed on https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

DOI: 10.15294/lesrev.v5i2.50601

The first principle consists of three parts. Lawfulness becomes the basis for whether the personal data obtained can be legally or not for processing.[25] Then regarding fairness referred to here is the whole collection process until the processing of personal data must not conflict with applicable law. Next is transparency. Transparency is always intended to be open to avoid the data subject's data being used, provided, disseminated, or sold to other parties, including to third parties, without the data subject's consent. To avoid this, data controllers must explain the mechanisms for collecting, processing, and storing personal data.[26]

Concerning the PeduliLindungi application, this application was issued on the legal basis of the Decree of the Minister of Communication and Informatics No. 171 of 2020 to help reduce the spread of the COVID-19 virus. In the privacy policy of personal data protection, PeduliLindungi has explained the collection to processing of personal data. PeduliLindungi obtains personal data when the data subject registers and consents when wishing to use the application. In addition, the personal data used have been described, such as location, camera access, and photos from media/files. In the mechanism of personal data protection, it has been explained that collecting, processing, and storing personal data is used for contact tracing to the storage of evidence of electronic certificates of vaccines.

However, one aspect has not explained the role between the Ministry of Communication and Informatics (Kominfo) and PT. Telkom Indonesia Tbk in the collection, processing, and storage of personal data and supporting the PeduliLindungi application. When viewed, Kominfo is a data controller and PT. Telkom Indonesia Tbk is a third party that has a legitimate relationship. But in the absence of transparency of the relationship and anything that can do between the data controller and third parties provides the potential for personal data stored to be transferred and used outside other purposes considering, as a telecommunications company, PT. Telkom Indonesia Tbk can use and utilize the data as the company's business needs and interests.

It can say that the PeduliLindungi application has carried out the first principle but has not been thoroughly done because the transparency section has not shown an explanation. For lawfulness and fairness has been done. But for the transparency part, especially the relationship with third parties, PT. Telkom Indonesia Tbk has not explained the relationship and purpose of using its data. The absence of transparency, making recently, personal data

[25]Harsha Perera, et. al. "Towards Integrating Human Values into Software: Mapping Principles and Rights of GDPR to Values", in *2019 IEEE 27th International Requirements Engineering Conference*, IEEE, 2019, p. 405.

[26] Ibid.

DOI: 10.15294/lesrev.v5i2.50601

stored in the PeduliLindungi application handed it over to the server of PT. Telkom Indonesia Tbk by using the domain of the analytic rock for use in several business units of PT. Telkom Indonesia Tbk.[27] This transparency is not clear, making the public as a data subject automatically ask what and why there is data transfer without the data subject's consent. Given data sensitivity, data controllers must pay attention to transparency's principle for good and not just as an advantage for others.[28]

2) Principle of Purpose Limitation

The second principle is to know what purpose personal data is to be collected. The principle of purpose limitation emphasizes that data collection must be known in advance so that it does not cause problems due to extensive data collection and misuse in the future.[29] It is expected that with the limitations of the purposes that have been carried out at the time of collection, the following process in the processing and storage of personal data can assess whether the data controller has been appropriate and responsible for the original purpose that has been submitted or vice versa. In the event of a difference in objectives, the data subject may determine that the data controller has committed a breach. Furthermore, the principle of limitation of purpose exists to guarantee the right to privacy to be protected, and data controllers are obliged to respect by complying with the transparency obligations described at the outset.[30]

The PeduliLindungi application was initially used to trace data subjects to find out people infected with the COVID-19 virus and updated to store electronic vaccine certificates. To date, PeduliLindungi has pursued the second principle regarding goal limitations. But recently, there has been a discourse that the PeduliLindungi application will become an e-wallet.[31] The reason is that PeduliLindungi will be widely downloaded and used by

---

[27] Anggoro Suryo Jati, "PeduliLindungi 'Setor Data' Ke Server Analitik Telkom?," Detik.com, 30 September 2021, accesed on https://inet.detik.com/security/d-5741855/pedulilindungi-setor-data-ke-server-analitik-telkom.

[28] Matthew Zook, Olle Jarv, and Tuuli Toivonen Age Poom "COVID-19 Is Spatial: Ensuring That Mobile Big Data Is Used for Social Good", *Big Data & Society*, Volume 7 Number 2, 2020, p. 5.

[29] Norjihan Abdul Ghani, Suraya Hamid, and Nur Izura Udzir "Big Data and Data Protection: Issues with Purpose Limitation Principle", *International Journal Advance Soft Computer Application*, Volume 8 Number 3, 2016, p. 119.

[30] Catherine Jasserand, "Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?", *European Data Protection Law Review*, Volume 4 Number 2, 2018, p. 22.

[31] Maya Citra Rosa, "Benarkah Aplikasi PeduliLindungi Akan Jadi Alat Pembayaran Digital?," Kompas.com, 30 September 2021, accesed on https://www.kompas.com/tren/read/2021/09/26/150000065/benarkah-aplikasi-pedulilindungi-akan-jadi-alat-pembayaran-digital-?page=all.

DOI: 10.15294/lesrev.v5i2.50601

hundreds of millions of people in the public room at the end of 2021. Not only that, the government has announced to integrate with 11 popular apps like Gojek, Grab, Tokopedia, Traveloka, Tiket, Dana, Livin' by Mandiri, Cinema XXI, LinkAja, Goers, and Jaki.[32] Multi-functional development is sure to experience serious challenges because it will connect the health sector and other sectors. If it is implemented, many parties are involved, and the potential for misuse of personal data will be even more significant.

In addition, the above discourse is less firmly based because it will happen otherwise where public confidence decreases. The argument is based on the current need to track communities in the face of the COVID-19 pandemic but will be used for other commercial purposes. Therefore, the government should consider limiting PeduliLindungi in the health sector to provide maximum personal data protection.

3) Principle of Data Minimisation

In the PeduliLindung application, personal data is used such as NIK, Name, Mobile Number, and Address. Then also request access with location and photo access from media/files. In the privacy policy it has been explained that the use of the requested personal data is used for contact tracing through location data. In the PeduliLindung application, personal data includes NIK, name, hp number, and address. Then also ask for access with location and photo access from media/files. The privacy policy has explained that the requested personal data use to trace through location data. In addition, photos from media/files are intended if the data subject will scan the barcode to open the camera in reading the barcode scanner to check in or check out when in the public room or travel and photos from the media/file are used to download electronic certificates of vaccines. That is, PeduliLindungi has carried out the principle of data minimization by using the personal data of data subjects whose use has been appropriate for current purposes.

4) Principle of Accuracy

This principle is the safeguarding in the event of a violation of the three regulations above described earlier, where suppose in the future found personal data that is not under the purpose of collection, processing, and storage. The personal data that have been used must be deleted immediately without delay.[33] The principle of accuracy aims to ensure and ensure that

---

[32] Cantika Adinda Putri, "Unduh 11 Aplikasi Ini, Pekan Depan Nyambung Ke PeduliLindungi," CNBC Indonesia, September 30, 2021, accesed from https://www.cnbcindonesia.com/tech/20211003134515-37-281013/unduh-11-aplikasi-ini-pekan-depan-nyambung-ke-pedulilindungi/amp.

[33] Diana Dimitrova, "The Rise of the Personal Data Quality Principle. Is It Legal and Does It Have an Impact on the Right to Rectification?," *SSRN*, October 1, 2021, accessed from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790602.

DOI: 10.15294/lesrev.v5i2.50601

public bodies or companies as data controllers can be accurate in processing personal data so that it runs reasonably. Furthermore, if there is impropriety, the data subject has the right to correct it so that it can demand the data controller to fix it, and the data controller must correct and update it to ensure the personal data is processed under the original purpose and still maintain the security of personal data.

In carrying out this principle, PeduliLindungi is widely highlighted when a vaccination certificate belonging to President Jokowi spreads on social media. There is a NIK and scan of vaccination barcodes.[34] The remedial action carried out by Kominfo as the controller is to directly close access to vaccine certificates belonging to President Jokowi and several other officials. The actions taken by Kominfo are under its capacity. Still, the Author sees that presidential data alone can be a hack, and other people's data also has excellent potential to be hacked. According to the Author, the closure of access should not only be given to officials but the public can be entitled to apply for closure so that the electronic certificate data of the vaccine is not used. This submission is under the principle of the right to correct in the principle of accuracy. The data subject reserves the right to request improvement from the data controller from open access to secure access. So far, PeduliLindungi is necessary to evaluate to create data accuracy to provide comfort and security for data subjects.

5) Principle of Storage Limitation

In addition to the delivery of collecting and processing personal data, no less important is how long the data controller wants to store the personal data of the data subject, in the case of the storage of personal data, no specified period or period.[35] It is just that the retention of personal data must not exceed what is necessary for achieving its purpose. So that after the purpose of storing personal data is complete, the personal data held is deleted. In assessing it, it will be connected with the sense and reasonableness of the accuracy of personal data storage.[36] Therefore, data controllers can assess and determine the storage of personal data from the beginning of the collection and processing of personal data. The goal is to avoid threats, given that the more comprehensive personal data is stored, the greater the potential it can be private to be misused.[37]

---

[34] Annisa Rizky Fadhila, "Sertifikat Vaksin Jokowi Tersebar, Ini 3 Hal Yang Diketahui Hingga Kini," Detik.com, 30 September 2021, accesed on https://news.detik.com/berita/d-5709033/sertifikat-vaksin-jokowi-tersebar-ini-3-hal-yang-diketahui-hingga-kini.

[35] Harsha Perera, et. al, Op. Cit, p. 407.

[36] Ibid.

[37] Ibid.

DOI: 10.15294/lesrev.v5i2.50601

What about archiving personal data by a data controller? Archiving still includes data storage, so the data controller must have a purpose for storing it.[38] If there is no purpose, the data controller is obliged to delete it because it is illegal to keep the data subject outside the specified or completed and unused time. The deletion of data is a right to be forgotten because effectively and to ensure that it prevents personal data from being misused. It expects that personal data cannot be reaccessed to do personal data protection done with this principle.[39]

This principle will store the personal data obtained in the data subject's mobile phone, periodically being sent to the PeduliLindungi server. After the data subject's personal data is stored in the PeduliLindungi server, then the deletion of personal data is done in several ways, including: 1) They are deleted periodically daily by the server after personal data is transmitted; 2) When the data subject deletes the application, the stored personal data will automatically be deleted; 3) The data subject may request individual deletion by submitting a request to delete personal data to the PeduliLindungi email. Furthermore, when the COVID-19 pandemic has complete, the personal data stored in the service will delete all personal data. Thus, the data controller of the PeduliLindungi application has provided clear storage restrictions in the storage of personal data related to the limitations of personal data storage.

6) Principle of Integrity and Confidentiality

The principle of integrity and confidentiality is intended for data controllers to implement the principle of personal data protection in processing to protect against unauthorized loss, misuse, access and disclosure, and alteration or destruction of personal data.[40] To carry it out, data controllers must have adequate security systems to prevent misuse of personal data during the processing or utilization of personal data. And be responsible in the event of unexpected losses or damages incurred to personal data. Therefore, every data controller must prepare technical security of personal data protection, proper human resources, have a robust system that is not easy to hack, and strive to protect from force majeure.

Related to this sixth principle is very closely related to the responsibility of data controllers. In terms of the use of PeduliLindungi, if there is a failure in the processing and storage of personal data that is not from the negligence of the data controller but arises due to the user's fault, then the data controller

---

[38] Eugenia Politou, et. al. "Backups and the Right to Be Forgotten in the GDPR: An Uneasy Relationship", *Computer Law & Security Review*, Volume 34 Number 6, 2018, p. 1247–1248.

[39] Ibid, p. 1248-1249.

[40] Borgesius Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen "The European Union General Data Protection Regulation: What It Is and What It Means", *Information & Communications Technology Law*, Volume 28 Number 1, 2019, p. 87.

DOI: 10.15294/lesrev.v5i2.50601

is free from responsibility. To apply this principle, the data controller has provided clauses regarding the use in the prohibited PeduliLndungi application and the technical security that data controllers perform in protecting the personal data of data subjects.

7) Principle of Accountability

The principle of accountability emphasizes that data controllers comply with all principles in the protection of personal data. This principle requires data controllers to show and demonstrate and document all activities of collecting, processing, and collecting personal data in strictly complying with the provisions of personal data protection law.[41] The end goal with the application of this principle is for data controllers to report and perform accountability. In addition to data controllers enforcing the principle of personal data protection, to assess what data controllers do, unique bodies are needed to supervise and ensure that data controllers have met the principles of personal data protection.[42] Special personal data protection agencies must audit, observe, and directly examine the application of personal data protection principles to avoid breaches by data controllers.[43]

In Indonesia, to apply this principle can be said to have not worked well, especially in the application of PeduliLindungi. This is because the authorized body and the one that handles personal data issues is Kominfo. Kominfo, as a supervisory agency here, then becomes confused because on the other hand Kominfo as its own data controller and audits itself against the collection, processing, and storage of personal data in the PeduliLindungi application. As a result, the enforcement of personal data protection cannot be maximized due to data controllers concurrently becoming supervisors. In addition to the absence of a unique body for personal data protection, DPO has not been implemented in Indonesia. Another reason has not been strong in the application of personal data protection principles.

Based on the analysis of the application of personal data protection principles in the PeduliLindungi application above, it can conclude that the collection, processing, and storage of personal data on the Application Of Protection is still not thoroughly carried out based on the principles of personal data protection due to weak supervision. Weak supervision is due to Indonesia not having a comprehensive personal data protection legal

[41] Christopher F. Mondschein and Cosimo Monda, "The EU's General Data Protection Regulation (GDPR) in a Research Context," in *Fundamentals of Clinical Data Science*, Springer International Publishing, Switzerland, 2019, p. 58.

[42] Ibid, p. 60.

[43] Ibid, p. 64.

DOI: 10.15294/lesrev.v5i2.50601

framework and the existence of the Personal Data Protection Agency and DPO so that the enforcement of personal data protection is still not vigorous. Seeing the current momentum with the era of big data and in the future, technology development will be faster. Indonesia must be ambitious to issue comprehensive regulations in providing a bulwark of privacy protection for its people's personal data.

The absence of regulations related to comprehensive personal data protection in Indonesia can assess weaknesses, indicating that Indonesia is not fully ready to enter the era of industrial revolution 4.0. This absence should be the focus and profound concern of the government to establish personal data protection regulations, given that comprehensive personal data protection regulations will support Indonesia's future development. In addition to supporting the future, complete personal data protection regulations put Indonesia on par with other countries in personal data protection.

B. The formulation on Development of Indonesia's Personal Data Protection Law in the Future

Looking at the point of view of personal data protection in Indonesia, there is still no unique and comprehensive regulation in the national legal system.[44] But in real terms, if viewed more deeply, Indonesia has personal data protection regulations, but it's still sectoral, spread across 17 regulations based on their respective fields.[45] The purpose of the spread of personal data protection regulations is still regulated separately in their fields, such as banking regulation, human rights, telecommunications, health, population administration, and electronic transactions.[46] The sectoral application makes the impression that so far, personal data protection has not been a severe problem, so it is considered a minor problem.[47] Unlike the EU, which has prepared and set a solid standard ambition in protecting personal data because it will be considered digital gold for the past few decades.[48] The

---

[44] Graham Greenleaf, *Asian Data Privacy Law: Trade and Human Rights Perspectives*, Oxford University Press, Oxford, 2017, p. 37.

[45] Erna Prilliasari, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online", *Majalah Hukum Nasional*, Volume 49 Number 2, 2019, hlm 146-148.

[46] Sinta Dewi Rosadi, "Balancing Privacy Rights and Legal Enforcement: Indonesian Practices", *International Journal of Liability and Scientific Enquiry*, Volume 5 Number 4, 2012, p. 233.

[47] Setyawati Fitri Anggraeni, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia", *Jurnal Hukum Dan Pembangunan*, Volume 48 Number 4, 2018, p. 823.

[48] Oskar Josef Gstrein, Op. Cit, p. 5.

DOI: 10.15294/lesrev.v5i2.50601

impact for Indonesia by not having comprehensive regulations, the enforcement of personal data protection seemed unable to show seriousness so far by looking at some cases of personal data leaks that have occurred because it is considered to have passed. If this is continuously allowed, it will automatically become a sovereignty threat to Indonesia itself in the future.[49]

Government measures as we advance must swiftly immediately pass a comprehensive personal data protection regulation. Because of the regulations spread and not one type, making the enforcement of personal data protection in Indonesia can not run optimally and automatically has not been able to protect the community. In this regard, when juxtaposed with the concept of legal protection, the state is obliged to provide preventive and repressive protection related to the integration of community interests.[50] So in achieving the protection of the law, it takes the development of regulations that lead to the interests of today's society.[51]

In achieving this, legal development is carried out by forming laws that should be important in the development agendas.[52] As described above, personal data has become valuable and needs to protect as part of the right to privacy. Therefore, it is necessary to prepare responsive regulations to protect personal data in Indonesia.[53] Considering that Indonesia is currently drafting and leaning into the EU in its preparation, it also needs a similar pattern to uphold the principles of personal data protection. The Author sees two things not regulated in the PDP Draft, namely the Personal Data Protection Agency and DPO. There are several reasons why the Personal Data Protection Agency and DPO are becoming crucial for protecting personal data in Indonesia.

1) Personal Data Protection Agency

---

[49] Russel Butarbutar, "Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia," in *3rd International Conference on Law and Governance*, Atlantis Press, 2019, p. 160.

[50] Philipus M. Hadjon, *Pengantar Hukum Administrasi Negara*, Gajah Mada Univesity Press, Yogyakarta, 2011, p. 279.

[51] M. Zulfa Aulia, "Hukum Pembangunan Dari Mochtar Kusumaatmadja: Mengarahkan Pembangunan Atau Mengabdi Pada Pembangunan?", *Jurnal Undang*, Volume 1 Number 2, 2018, p. 370–371.

[52] Mochtar Kusumaatmadja, *Konsep-Konsep Hukum Dalam Pembangunan*, PT Alumni, Bandung, 2012, p. 88.

[53] H.R. Benny Riyanto, "Pembangunan Hukum Nasional Di Era 4.0", *Rechtsvinding*, Volume 9 Number 2, 2020, p. 179.

DOI: 10.15294/lesrev.v5i2.50601

The vital role of the existence of the Personal Data Protection Agency is to ensure compliance and to promote adequate protection of personal data. The presence of a Personal Data Protection Agency will confirm can apply the protection of personal data responsibly.[54] In addition, the existence of the Personal Data Protection Agency is a crucial factor in the implementation of personal data protection policies and the raising of awareness, consultation, and networking.[55] Therefore, the existence of this body is vital because it can obtain and disseminate adequate knowledge about new technological developments in personal data protection practices to ensure security both now and in the future.[56]

A concrete example is the EU in anticipating surveillance in the form of contact tracing applications that at the beginning of the emergence of the COVID-19 pandemic issued technical and stricter regulations by EPDB to keep applying the principles of personal data protection, namely Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak. Indirectly, the EU GDPR as a comprehensive and rigorous regulatory system has proven successful in supporting the principles under Article 5 of the EU GDPR in the face of the COVID19 pandemic.[57] EPDB will ensure that each country exercises all personal data protection principles and requires developers of new or existing technologies to implement privacy-friendly options from the start (privacy by design and default).[58]

There are several options for establishing a Personal Data Protection Agency whose model depends on the needs of each country. In the case of Indonesia, it can apply several scenarios. First, use a single model of authority by creating new institutions. Second, it uses a dual authority model by bringing together nearby institutions and remaining independent. The

---

[54] Peter Hustinx, "The Role of Data Protection Authorities," in *Reinventing Data Protection?*, Springer International Publishing, Switzerland, 2009, p. 131.

[55] M Szydło, "Principles Underlying Independence of National Data Protection Authorities: Commission v. Austria", *Common Market Law Review*, Volume 50 Number 6, 2013, p. 1812.

[56] C. Raab and I Szekely, "Data Protection Authorities and Information Technology", *Computer Law & Security Review*, Volume 33 Number 4, 2017, p. 421.

[57] Laura Bradford, Mateo Aboy and Kathleen Liddell, "COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes", *Journal of Law and the Biosciences*, Volume 7 Number 1, 2020, p. 3.

[58] Rehana Harasgama and Gil Scheitlin Gemma Newlands, Christoph Lutz, Aurelia Tamo`-Larrieux, Eduard Foschi Villaronga, "Innovation Under Pressure: Implications for Data Privacy During the Covid-19 Pandemic", *Big Data & Society*, Volume 7 Number 2, 2020, p. 2.

DOI: 10.15294/lesrev.v5i2.50601

selection of an independent body of institutions based on the dimensions of personal data that have broad aspects and avoid conflicts of interest. Several indicators determine the independence of personal data protection bodies. Independence should be seen in terms of institutional independence, commissioner independence, human resources independence, organizational independence, and financial control.[59]

2) Data Protection Officer (DPO)

When implemented, the system at each data controller is assisted by an official acting as a personal data protection officer to perform electronic identification and electronic authentication when reporting and updating personal data.[60] A DPO is an official appointed and employed in a public agency or company to oversee regulations on personal data protection. Therefore, those responsible for protecting personal data should evaluate what is collected and processed by the authorities for what purposes and where it is the location for security reasons. In addition, data protection officers have a particular interest in contracts with processors that contain verifiable service levels concerning IT, cloud, and other systems.[61]

DPO here acts as an official or agent that regulates the procedures for protecting personal data for public bodies or companies. DPO must have professional qualities in carrying out its duties, particularly knowledge of the law and practice of personal data protection and ability of the economy and control organizations.[62] DPO itself plays an essential role as a key to strengthening public responsibility and trust around personal data protection.[63] In addition to those mentioned earlier, the DPO also plays on the principle of accountability to ensure compliance with personal data protection regulations, including cultural changes that support transparent data protection, privacy and user control policies, internal clarity, and enforcement

---

[59] Wahyudi Jafar and M. Jodi Santoso, *Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen*, ELSAM, Jakarta, 2019, p. 25.

[60] Paul Lambert, *The Data Protection Officer: Profession, Rules, and Role*, CRC Press, New York, 2016, p. 154.

[61] Ibid.

[62] Muhammad Iqsan Sirie, "The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law", *Padjadjaran Journal of Law*, Volume 5 Number 1, 2018, p. 30.

[63] Miguel Recio, "Data Protection Officer: The Key Figure to Unsure Data Protection And Accountability", *European Data Protection Law Review*, Volume 3 Number 1, 2017, p. 117.

DOI: 10.15294/lesrev.v5i2.50601

procedures.[64] The importance of DPO for Indonesia is based on looking at Tokopedia data breach cases where Indonesia's data protection law has not determined between the obligations and accountability of data controllers in applying personal data protection principles.[65] References with the DPO will further explain whether the data controller has applied the personal data protection principle or vice versa.[66] The above two points that have to present will make the umbrella of personal data protection law in Indonesia more comprehensive because personal data protection laws will increase when handled by controllers (DPO) and regulatory bodies.[67]

4. CONCLUSION

The application of personal data protection principles in the PeduliLindungi application has not been fully implemented, mainly in the principle of transparency, data minimization, and limitation of purpose. The factor that causes the lack of application of personal data protection principles in the PeduliLindungi application is the absence of comprehensive personal data protection regulations in Indonesia so that Kominfo currently doubles as a personal data controller as well as a personal data supervisor. Automatically, in the absence of comprehensive regulation and the occurrence of a dual role by Kominfo, the enforcement of personal data protection principles in Indonesia has not been able to run optimally. In the future, Indonesia must immediately ratify comprehensive personal data protection regulations by establishing a special Personal Data Protection Agency and DPO to create supervision of personal data protection principles and stronger.

5. DECLARATION OF CONFLICTING INTERESTS

None

---

[64] Mehmet Bedii Kaya, "The New Paradigm of Data Protection Law: The Principle of Accountability", *Istanbul Law Review*, Volume 78 Number 4 , 2020, p. 1861.

[65] Alvansa Vickya and Reshina Kusumadewi, "Kewajiban Data Controller Dan Data Processor Dalam Data Breach Terkait Pelindungan Data Pribadi Berdasarkan Hukum Indonesia Dan Hukum Singapura: Studi Kasus Data Breach Tokopedia", *Padjadjaran Law Review*, Volume 9 Number 1, 2021, p. 14–15.

[66] European Commission, "What Are the Responsibilities of a Data Protection Officer (DPO)?," 29 September 2021, accessed on https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en.

[67] Claudia Quelle, "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach", *European Journal of Risk Regulation*, Volume 9 Number 3, 2018, p. 502.

DOI: 10.15294/lesrev.v5i2.50601

6. FUNDING INFORMATION

None

7. ACKNOWLEDGEMENTS

My deepest thanks to Mrs. Umi Khaerah Pati, S.H., M.H., who has guided and provided outstanding support to the author to complete this article.

8. REFERENCES

Age Poom, Olle Jarv, M. Z. and T. T. (2020). COVID-19 is Spatial: Ensuring that Mobile Big Data is Used for Social Good. *Big Data & Society*, *7*(2), 5.

Aihara, N. H. and Y. (2017). Data Privacy Protection of Personal Information Versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan). *Defense Council Journal*, *84*(1), 1.

Anggraeni, S. F. (2018). Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum di Indonesia. *Jurnal Hukum Dan Pembangunan*, *48*(4), 823.

Aulia, M. Z. (2018). Hukum Pembangunan dari Mochtar Kusumaatmadja: Mengarahkan Pembangunan atau Mengabdi Pada Pembangunan? *Jurnal Undang*, *1*(2), 370–371.

B. Sowmiya, V.S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. T. & P. V. (2021). A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19. *SN Computer Science*, *2*(136), 4.

Bradford, L., & Liddell, M. A. and K. (2020). COVID-19 Contact Tracing Apps: a Stress Test for Privacy, the GDPR, and Data Protection Regimes. *Journal of Law and the Biosciences*, *7*(1), 3.

Bratajaya, A. K. S. and Y. (2020). Contact Tracing Apps in Asean : A Threat to Privacy and Personal Data. *Kathmandu School of Law Review*, *8*(1), 53.

Budhijanto, D. (2019). *Cyber Law dan Revolusi Industri 4.0*. Bandung: Logoz Publishing.

Butarbutar, R. (2019). Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia. *3rd International Conference on Law and Governance*, 160. Atlantis Press.

Chris Jay Hoofnagle, Bart van der Sloot, and F. Z. B. (2019). The European Union General Data Protection Regulation: What it is and What it Means. *Information & Communications Technology Law*, *28*(1), 87.

Denindah Olivia, Sinta Dewi Rosadi, dan R. R. P. (2020). Perlindungan Data

Pribadi Dalam Penyelenggaraan Aplikasi Surveilans Kesehatan Pedulilindungi dan Covidsafe di Indonesia dan Australia. *Datin Law Journal*, *1*(2), 14.

Dimitrova, D. (2021). The Rise of the Personal Data Quality Principle. Is it Legal and Does it Have an Impact on the Right to Rectification? *SSRN*, 3–4. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790602

Eugenia Politou, et. al. (2018). Backups and the Right to be Forgotten in the GDPR: An Uneasy Relationship. *Computer Law & Security Review*, *34*(6), 1247–1248.

European Commision. (2021). What are the responsibilities of a Data Protection Officer (DPO)? September 29, 2021, accessed from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en

European Data Protection Board. (2021). Opinion 32/2021 regarding the European Commission Draft Implementing Decision according to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the Republic of Korea. September 28, 2021, accessed from https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en

Fadhila, A. R. (2021). Sertifikat Vaksin Jokowi Tersebar, Ini 3 Hal yang Diketahui Hingga Kini, accesed on Detik.com, September 30, 2021, accesed from https://news.detik.com/berita/d-5709033/sertifikat-vaksin-jokowi-tersebar-ini-3-hal-yang-diketahui-hingga-kini

Gemma Newlands, Christoph Lutz, Aurelia Tamo`-Larrieux, Eduard Foschi Villaronga, R. H. and G. S. (2020). Innovation Under Pressure: Implications for Data Privacy During the Covid-19 Pandemic. *Big Data & Society*, *7*(2), 2.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703.

Gray, N. R. and D. (2020). Mass Surveillance in the Age of COVID-19. *Journal of Law and the Biosciences*, *7*(1), 17.

Greenleaf, G. (2017). *Asian Data Privacy Law: Trade and Human Rights Perspectives*. Oxford: Oxford University Press.

Gstrein, O. J. (2021). The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment. *European Journal of Risk Regulation*, *12*(2), 8.

Hadjon, P. M. (2011). *Pengantar Hukum Administrasi Negara*. Yogyakarta: Gajah

DOI: 10.15294/lesrev.v5i2.50601

Mada Univesity Press.

Harsha Perera, et. al. (2019). Towards Integrating Human Values into Software: Mapping Principles and Rights of GDPR to Values. *2019 IEEE 27th International Requirements Engineering Conference*, 405.

Hino, R. A. F. dan A. (2020). COVID-19, Digital Privacy, and the Social Limits on Data-focused Public Health Responses. *International Journal of Information Management*, *55*, 1.

Hustinx, P. (2009). The Role of Data Protection Authorities. In *Reinventing Data Protection?* (p. 131). Switzerland: Springer International Publishing.

Ibrahim, J. (2006). *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayu Media Publikasi.

Jaccard, J. J. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973.

Jasserand, C. (2018). Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation? *European Data Protection Law Review*, *4*(2), 22.

Jati, A. S. (2021). PeduliLindungi "Setor Data" ke Server Analitik Telkom? Detik.com, 30 September 2021, accesed on https://inet.detik.com/security/d-5741855/pedulilindungi-setor-data-ke-server-analitik-telkom

Kaya, M. B. (2020). The New Paradigm of Data Protection Law: The Principle of Accountability. *Istanbul Law Review*, *78*(4), 1861.

Kletter, J. A. and R. (2018). *Artificial Intelligence: Confronting The Revolution*. California: Endeavour Media Ltd.

Kusumaatmadja, M. (2012). *Konsep-Konsep Hukum dalam Pembangunan*. Bandung: PT Alumni.

Kusumadewi, A. V. and R. (2021). Kewajiban Data Controller dan Data Processor Dalam Data Breach Terkait Pelindungan Data Pribadi Berdasarkan Hukum Indonesia dan Hukum Singapura: Studi Kasus Data Breach Tokopedia. *Padjadjaran Law Review*, *9*(1), 14–15.

Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. New York: CRC Press.

Larry Ozeran, Anthony Solomonides, and R. S. (2021). Privacy versus Convenience: A Historical Perspective, Analysis of Risks, and an Informatics Call to Action. *Applied Clinic Informatics*, *12*(2), 274.

Molla Rashied Hussein, Abdullah Bin Shams, Ehsanul Hoque Apu, Khondaker Abdullah Al Mamun, dan M. S. R. (2020). Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations. *2nd International Conference on*

Advanced Information and Communication Technology, 1–2. IEEE.
Monda, C. F. M. and C. (2019). The EU's General Data Protection Regulation (GDPR) in a Research Context. In *Fundamentals of Clinical Data Science* (p. 64). Switzerland: Springer International Publishing.
Norjihan Abdul Ghani, Suraya Hamid, and N. I. U. (2016). Big Data and Data Protection: Issues with Purpose Limitation Principle. *International Journal Advance Soft Computer Application*, *8*(3), 119.
Nurhidayati, Sugiyah, dan K. Y. (2021). Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi. *Widya Cipta: Jurnal Sekretari Dan Manajemen*, *5*(1), 44.
Paariadi, D. (2018). Pengawasan E-Commerce dalam Undang-Undang Perdagangan dan Undang-Undang Perlindungan Konsumen. *Jurnal Hukum Dan Pembangunan*, *48*(3), 653.
Prilliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, *49*(2), 25.
Pujiyono, Kukuh Tejomurti, Pranoto, dan U. K. P. (2020). The Principle of Proportionality in Using Smart City Cloud Computing For Patients Privacy Rights Protection in Handling the Covid-19 Pandemic. *Solid State Technology*, *63*(4), 1122.
Putri, C. A. (2021). Unduh 11 Aplikasi Ini, Pekan Depan Nyambung ke PeduliLindungi. CNBC Indonesia, 30 September 2021, accessed on https://www.cnbcindonesia.com/tech/20211003134515-37-281013/unduh-11-aplikasi-ini-pekan-depan-nyambung-ke-pedulilindungi/amp
Quelle, C. (2018). Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation*, *9*(3), 502.
Recio, M. (2017). Data Protection Officer: The Key Figure to Unsure Data Protection And Accountability. *European Data Protection Law Review*, *3*(1), 117.
Riahi, Y. (2015). Big Data and Big Data Analytics: Concept, Types and Technology. *International Journal of Research and Engineering*, *5*(9), 525.
Riyanto, H. R. B. (2020). Pembangunan Hukum Nasional di Era 4.0. *Rechtsvinding*, *9*(2), 179.
Rosadi, S. D. (2012). Balancing Privacy Rights and Legal Enforcement: Indonesian Practices. *International Journal of Liability and Scientific Enquiry*, *5*(4), 233.
Rosadi, S. D. (2016). Implikasi Penerapan Program E-Health Dihubungkan dengan Perlindungan Data Pribadi. *Arena Hukum*, *9*(3), 418.
Rosa, M. C. (2021). Benarkah Aplikasi PeduliLindungi akan Jadi Alat

Pembayaran Digital? Kompas.com, September 30, 2021, accesed from https://www.kompas.com/tren/read/2021/09/26/150000065/benarkah-aplikasi-pedulilindungi-akan-jadi-alat-pembayaran-digital-?page=all

Santoso, W. J. and M. J. (2019). *Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen*. Jakarta: ELSAM.

Sirie, M. I. (2018). The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law. *Padjadjaran Journal of Law*, *5*(1), 30.

Szekely, C. R. and I. (2017). Data Protection Authorities and Information Technology. *Computer Law & Security Review*, *33*(4), 421.

Szydło, M. (2013). Principles Underlying Independence of National Data Protection Authorities: Commission v. Austria. *Common Market Law Review*, *50*(6), 1812.

Taddeo, M. (2020). The Ethical Governance of the Digital During and After the COVID-19 Pandemic. *Minds and Machines*, *30*, 171.

Tiara Almira Raila, Sinta Dewi Rosadi, dan R. R. P. (2020). Perlindungan Data Privasi di Indonesia dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan COVID-19 dan Tanggungjawabnya. *Jurnal Kepastian Hukum Dan Keadilan*, *2*(1), 14.

Trotogott, R. L. (2020). A Comparative Analysis of Data Privacy Impacted by Covid-19 Contact Tracing in the European Union, the United States, and Israel: Sacrificing Civil Liberties for a Public Health Emergency. *ILSA Journal of International & Comparative Law*, *27*(1), 70.

DOI: 10.15294/lesrev.v5i2.50601

ABOUT AUTHOR(S)

Anugrah Muhtarom Pratama, commonly called Tama is a student of the Faculty of Law, Universitas Sebelas Maret. Tama is currently actively a staff member of the Research Division in Kelompok Studi Penelitian "Principium" (KSP "Principium") Faculty of Law, Universitas Sebelas Maret.

Umi Khaerah Pati is a lecturer of Civil Law, the Faculty of Law, Universitas Sebelas Maret.

DOI: 10.15294/lesrev.v5i2.50601