

Human Security Principles in Crowdsourcing Personal Data

Dona Budi Kharisma¹, Agus Yudha Hernoko², Prawitra Thalib³, Oktafiyana⁴
donabudikharisma@staff.uns.ac.id¹, yudha@fh.unair.ac.id²,
prawitra@fh.unair.ac.id³, oktafiyana@student.uns.ac.id⁴

Faculty Of Law, Universitas Sebelas Maret, Indonesia^{1,2,3}

Faculty Of Law, Universitas Airlangga, Indonesia⁴

Article Info

Received: 2024-05-10

Revised: 2024-09-06

Accepted: 2024-12-30

Keywords:

Crowdsourcing, human security principle, personal data protection, economy digital.

Abstract

Personal data protection is fundamental because every individual's privacy is important. This article analyses related principles of human security in the context of processing personal data to ensure the safety of every personal data subject. The result of the paper shows that every effort in processing personal data must based on principles to ensure the fulfillment of human security principles. This article argues that crowdsourcing personal data often carried out in the digital era violates human security principles when impact losses are incurred to man

I. Introduction

Privacy is the right of an individual to control himself, which is the constitutional core dignity of man.¹ Privacy data is things that don't can separated from personal data protection. Every individual has the right to mandatory privacy and security. Privacy is part of the right because privacy is essential for everyone.² There are three principles related to ownership, Edmon Makarim stated that privacy is a right not to disturb other people's personal lives, the right to keep secret information about nature-sensitive

¹ Payal Thaorey, "Legal Intropection Towards The Development of Right to Privacy as Fundamental Right in India" *Indonesia Law Review* 11, no. 3 (2021): 310.

² Princess Alafaa, "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World.," *SSRN Electronic Journal*, 2022, 2, <https://doi.org/10.2139/ssrn.4005750>.

matters, and the right to control the use of personal data by other parties.³

In This digital era, security from personal data is essential because the data is accessible to save and send.⁴ In 2022, internet users worldwide are estimated to reach 5.3 billion.⁵ That indicates that much processing of personal data occurs due to the digital era. This public must deposit their data to use online register applications or services. They submit personal data based on the agreement by the terms and conditions attached to the party organizer application. Society wants it for existing privacy, but consciously, they share personal data. Therefore, it is necessary to supervise and change how personal data is processed.⁶

A class action lawsuit filed by WH Law against Roblox in America represents the importance of personal data protection moment. Regarding these users, most Roblox applications are children who feel cheated into giving personal information and biometric data to the company. WH Law filed a class action lawsuit to protect children's privacy in Illinois, a state in the United States. Roblox encourages children to provide biometric data the moment they register and can utilize services that are provided for playing the game, even though, on the other hand, the law Privacy Information Biometrics Illinois ("BIPA") states that company no can collect, store, or provide "biometric data" which includes things like scanning face or fingerprint finger, without notification and approval moreover formerly. WH Law believes that Roblox uses technology introduction face to make a unique template that can be used to identify the user through photos, which is a matter. This violates the provision from BIPA.⁷

Security of personal data is essential for protection because of the proper privacy. In 2019, TikTok was sued by parents in the United States. When registering an application, every user will submit personal data, but personal data can only be used simply for existing needs approved by the user. In terms of this, TikTok allegedly takes information about individual children's user applications without agreement through legal and without knowledge from parents and children.⁸ The demands are submitted, and the data is

³ Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik* (Jakarta: Rajawali Pers, 2010), 298–99.

⁴ Marc Pelteret and Jacques Ophoff, "A Review of Information Privacy and Its Importance to Consumers and Organizations," *Informing Science: The International Journal of an Emerging Transdiscipline* 19 (2016): 1, <https://doi.org/10.28945/3573>.

⁵ Statista, "Internet and Social Media Users in the World 2023," Statista, accessed November 13, 2023, <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

⁶ Dona Budi Kharisma and Alfiya Hunaifa, "Comparative study of disgorgement and disgorgement fund regulations in Indonesia, the USA and the UK", *Journal of Financial Crime*, 30(3) 2022, pp. 635–649. Available at: <https://doi.org/10.1108/JFC-01-2022-0022>.

⁷ Brandon Haubert, "Roblox Is Stealing Your Kids Biometric Data," wh Law, February 15, 2022, <https://whlawoffices.com/blog/roblox-is-stealing-your-kids-biometric-data/>.

⁸ "TikTok sued for billions over use of children's data," *BBC News*, April 21, 2021, sec. Technology, <https://www.bbc.com/news/technology-56815480>.

retrieved in a way that is veiled and sent to Chinese servers.⁹

Weak supervision of the processing of personal data causes the emergence of possible problems and harms every subject personally. In 2018, several successful British media proved that Cambridge Analytica (CA), a consulting company in politics and data analysis, had committed crimes regarding personal data.¹⁰ The company stores 87 million individual data users for interest unilaterally without agreement from the personal data subject.¹¹ According to the settings listed in Article 6 of the General Data Protection Regulation, the processing of personal data can be done if the topic of personal data gives consent or if permitted by law. Violation right CA's privacy practices are known for winning Donald Trump by the way they built software using 87 million personal data users on Facebook for prediction and influence options in the box voice.¹²

In 2020, something happened during a case data leak from a user Tokopedia e-commerce application. Hackers stole data from 91 million account users and 7 million merchant accounts. Data taken includes email, password, and name of user.¹³ Then, the hacker sells the stolen data for US\$ 5,000.¹⁴ The data leak phenomenon is related to personal data, which is an asset of high economic value.¹⁵ However, this violated every sense of security right owned by individuals below his power.¹⁶ Respect for individuals is part of the rights protected by the concept of privacy.¹⁷ Problems regarding personal data will arise along with the ability to use digital technology and continuous networking to develop his abilities to collect, store, and analyze data. Use social media applications or online services because of existing processing of personal data. So, crowdsourcing is a part of life in this digital era. It is known that the principle of human security ensures that the safety of every individual still notices every processing of personal data.

⁹ Siladitya Ray, "Class Action Lawsuit Alleges TikTok 'Collected Data From Minors, Sent It To Servers In China,'" *Forbes*, accessed November 28, 2023, <https://www.forbes.com/sites/siladityaray/2020/08/05/class-action-lawsuit-alleges-tiktok-collected-data-from-minors-sent-it-to-servers-in-china/>.

¹⁰ Maya Bofa, Darmawan Wawan Budi, and Arifin Sudirman, "Data Rights di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook dalam Pemilihan Presiden Amerika Serikat 2016," *Hasanuddin Journal of International Affairs* 2, no. 2 (November 27, 2022): 144–59, <https://doi.org/10.31947/hjirs.v2i2.22686>.

¹¹ Olivia Goldhill, "A 'big data' firm sells Cambridge Analytica's methods to global politicians, documents show," *Quartz*, August 14, 2019, <https://qz.com/1666776/data-firm-ideia-uses-cambridge-analytica-methods-to-target-voters>.

¹² Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, sec. News, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

¹³ Muhammad Raihan, "Perlindungan Data Diri Konsumen dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)," *Jurnal Inovasi Penelitian* 3, no. 10 (March 2023): 7848.

¹⁴ "Complete Chronology of 91 Million Tokopedia Accounts Leaked and Sold," accessed December 12, 2023, <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>.

¹⁵ Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: PT. Raja Grafindo Perkasa, 2003), 3.

¹⁶ Dona Budi Kharisma, "Urgency of Financial Technology (Fintech) Laws in Indonesia", *International Journal of Law and Management*, 63(3), 2021, pp. 320–331. Available at: <https://www.emerald.com/insight/content/doi/10.1108/IJLMA-08-2020-0233/full/html>

¹⁷ Larry M. Ellison, "Right of Privacy," *Montana Law Review* 48, no. 1 (January 1987).

The application principle of human security started from the adopted resolution UN General Assembly 66/290 of 10 September 2012. The General Assembly approved the approach of security men in the UN system.¹⁸ Principle human security Alone refers to the concept of security that focuses on protecting the welfare of humans, not only from physical threats but also non-physical threats like violation of privacy and misuse of personal data. Sharbanaou Tadjbakhsh and Anuradha M. Chenoy define human security as protection for every individual from all threatening things security physique as well as dignity.¹⁹ So, it has already become an obligation to apply the principle of human security in the digital era.

Principle human security very tightly about personal data because personal data collection can give rise to privacy and security individual risks. The crowdsourcing as digital power is often used as a road to go out when a problem is solved. A computer can complete no, so it is necessary an ability man. Without notice, the principle of human security, the collection of personal data through crowdsourcing can result in misuse of data, breach of privacy, and risk to the safety of others who can harm the individual.

Along with the previous arguments, the article arranged to answer problems related to principles human security and several possible questions arise related to crowdsourcing personal data. Firstly, will analyze the related code of human security in the context of personal data protection. The second chapter will elaborate on how the crowdsourcing mechanism violates the human security principle. This article studies the crowdsourcing of personal data in personal data protection to highlight whether crowdsourcing violates the principle of human security.

2. Research Method

This research uses a statute approach. In the statute approach, the object of research is the Act related to the legal issue being studied.²⁰ Acts used:

- a. Indonesian Electronic Information and Transactions Act Number 11/2008, as amended by Act Number 19/2016;
- b. Indonesian Personal Data Protection Act Number 27/2022 (PDPA Indonesia);
- c. General Data Protection Regulation (GDPR);
- d. Malaysian Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia).
- e. Hong Kong's Personal Data Protection Ordinance (PDPO) of 2021 (PDPO Hong Kong);
- f. Europe Union Data Protection Directive.

¹⁸ United Nations, Human Security Handbook, 2016, 6.

¹⁹ Shahrbanou Tadjbakhsh and Anuradha Chenoy, *Human Security: Concepts and Implications*, 1st ed. (London: Routledge, 2007).

²⁰ Peter Mahmud Marzuki, "Penelitian Hukum (Cetakan Ke-14)", Jakarta: Prenada Media Group: Divisi Kencana, 2019.

3. Results and Discussion

Human Security Principles in Processing of Personal Data

The development of the times brings life experience renewal in a digital direction.²¹ Digitalization in field communication makes the digital realm closely related to security man as the user. The principle of human security emphasizes the protection of individuals, not only the state and the business world.²² A development based on individual society, then Already must everyone feel safe on income, employment, and resources his livelihood, as well as spared from threat or social conflict.²³ So, deep matter this embodiment of personal data protection must be based on the principle of human security to protect the rights of individuals and the public. Personal data protection is attached to the application principle of human security.

The principle of human security that focuses on society makes matters the focus on protecting individuals. One important pillar in the protection of individuals is tied to the protection of personal data. So, what is needed is to respond to how the public sector's data protection faces various threats, abuse, and things that can harm individual data subjects, whether in the form of material or immaterial. Through the principle of human security, personal data protection is focused on privacy. Everyone can be protected and have the right to authority over their data so that no one can access or process the data.

Personal data can be misused for various dangerous activities security for personal data is subject to the. Infringing on the private data provisions can harm individual data subjects, which can happen when personal data is used for criminal actions like theft of personal data. That matter naturally results in a loss for every individual data subject. Apart from the disadvantages, the security of personal data is threatened because data can be misused for criminal purposes. Therefore, every processing of personal data must be based on the principle of human security. To ensure the safety of personal data, the subject is the holder of the right authority over personal data.

In the first draft, personal data protection centered on guarding confidentiality against individual data, along with developments in data processing, have brought great influence to the enhancement of the protection rights of individuals.²⁴ In the processing of personal data, there is a must aspect complied with by the personal data processor, which constitutes the party processing personal data on Name personal data controller. To

²¹ Dona Budi Kharisma. "Membangun Kerangka Pengaturan Startup di Indonesia", Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, [S.l.], v. 10, n. 3, p. 431-445, dec. 2021. ISSN 2580-2364. doi: <http://dx.doi.org/10.33331/rechtsvinding.v10i3.766>

²² Darang S Candra and Broto Wardoyo, "Implementing Human Security Measures in the Cyberspace: Navigating through the Institutional and Regulatory Disarray," n.d., 4.

²³ Bo Asolund and Romeo Reyes, "Human Security, Human Development, and The Millenium Development Goals" *Indonesian Journal of International Law* 1, no. 1 (August 12, 2021): 38, <https://doi.org/10.17304/ijil.vol1.1.168>.

²⁴ Daniar Supriyadi, "The Regulation of Personal and Non-Personal Data in the Context of Big Data," *Journal of Human Rights, Culture and Legal System* 3, no. 1 (February 14, 2023): 36, <https://doi.org/10.53955/jhcls.v3i1.71>.

ensure a principle of human security for every individual data subject. Various company moments This is confronted with risk-related data breaches that impact the company, such as Facebook, LinkedIn, and Wells Fargo. Therefore it is important to guard data security that focuses on the data collected and processed so that it is not hacked or used by parties who are not interested.²⁵

The processing of personal data must based on the implementation principle of human security. Application principle that can be fulfilled in a way that obeys rules in processing personal data for guard security from every personal data subject. Article 5 of the European Union General Data Protection Regulation (GDPR) explains that in processing personal data, there are basic: legitimacy, fairness, and transparency; goal limitations; data minimization; accuracy; limitation storage; and integrity and confidentiality.

Legitimacy, fairness, and transparency in processing personal data ensure that every processing is carried out fairly, with valid reasons, and transparently to every personal data subject. Inner validity matters. This means every processing of personal data is done based on a provision governing law. In this case all processing of personal data can't be contrary to the rules and applicable law. When conveying this violates applicable legal regulations, it can be said to be a threat to human security. Because data subjects are vulnerable to exploitation, user consent is required to make a personal data processing practice considered legal. When storing personal data, safety must be emphasized for each individual based on the principle of human security, where the collection and collection of personal data must be based on law, namely the existence of consent, contractual requirements, compliance with legal obligations, protection of vital interests or the public interest.²⁶

Maker policy, industry, or academics require that it processes personal data fairly, which is the underlying standard aspect of data protection.²⁷ Justice in processing personal data can be reviewed from the origin of the data obtained wandering and without agreement from the personal data subject or obtained fairly and with no harm to the party's individual data subject. When personal data is obtained without agreement from the data owner, it can be said to violate human security because, without an existing deal from the data owner, it is the same as bother from the security data owner. This matter is due to personal data being owned by the attached personality of every individual. So that every personal data subject is entitled to their rights, and if exactly violated, they allowed demands based on law-related loss of material or perceived immaterial.

²⁵ Paola Estrada, "Global Data Privacy Practices and the Importance of Privacy Awareness in Today's Virtual Realm," *SSRN Electronic Journal*, 2022, 4, <https://doi.org/10.2139/ssrn.4118695>.

²⁶ "Data Protection and Privacy Laws | Identification for Development," accessed December 3, 2023, <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>.

²⁷ Damian Clifford and Jef Ausloos, "Data Protection and the Role of Fairness," *CiTiP Working Paper 29/2017*, August 2017, 5.

The processing of personal data must behave transparently so that every individual data subject knows What will be done to personal data. Every personal data subject is entitled to know What will be done regarding personal data because they are transparent and objective. This will guard security from individual data subjects. Personal data subjects also have the right to know who is processing their data. That matter is done to guarantee a sense of security to rights owned by personnel from personal data subjects. Principle of human security in this case protects all interest data owners so as not to be disadvantaged because they are entitled to transparency in processing personal data. Every personal data subject, as well as later, must easily access related information about processing their data.²⁸

Restrictions are objective in processing personal data to protect the security of everyone. As conditions are objective, individual data processors can't arbitrarily process personal data. This collection of personal data is done for goals that have been agreed upon or not permitted for processed outside matters. Restriction objective is useful in ensuring data processors know exactly what data they need so that every data processor understands the related impact of activity processing the data.²⁹

The principle of human security emphasizes that personal data must protected, that must be protected goal is irrelevant or not permitted. Through restrictions, objective processing of personal data must have a specific purpose per the agreement for the security and privacy of personal data subjects. That individual data is protected will strengthen the application principle of human security inside personal data protection. Processing more carry-on personal data objective scientific or statistics can fulfill principle restrictions purpose; however, it must satisfy aspect protection to the individual data subject.³⁰

Restrictions objective can ensure form certainty law from exists A processing of personal data because it exists restrictions objective so all processes carried out No can outside what has been agreed. If deep implementation processing of personal data, there is a change in which goal is different from the goal at the beginning that has been approved, so it must be assessed formerly related aspects of compatibility. The matter must notice several aspects, i.e., the connection between the objective starting with a new goal, context of data collection, nature of data, impact on personal data subjects, and protection.³¹ Such

²⁸ Robert Healey, "The Principle of Lawfulness, Fairness, and Transparency," Formiti, October 23, 2023, <https://formiti.com/data-privacy-the-principle-of-lawfulness-fairness-and-transparency/>.

²⁹ Griet Verhenneman, *The Patient, Data Protection and Changing Healthcare Models: The Impact of e-Health on Informed Consent, Anonymisation and Purpose Limitation*, KU Leuven Centre for IT & IP Law Series (Cambridge: Intersentia, 2021).

³⁰ Nikolaus Forgó, Stefanie Hännold, and Benjamin Schütze, "The Principle of Purpose Limitation and Big Data," in *New Technology, Big Data and the Law*, Perspectives in Law, Business and Innovation (Singapore: Springer, 2017), 39.

³¹ "Can We Use Data for Another Purpose?," accessed December 3, 2023, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en.

things are done to uphold the principle of human security, which is prioritized for the safety of every individual private data owner.

Prioritizing personal data protection aspect human security is also a must-notice related to deep data minimization matter processing of personal data. Data minimization makes data collection for personal data focus on goal processing. Then, unique data is required according to the purpose: what can be collected and processed. Personal data must be relevant, adequate, and limited according to what becomes objective. Individual data processors must be wise in using existing data collected because of concerns about the owner's privacy. In terms of This, personal data processors must pay attention to what data must be collected and whether it is relevant to the purpose. So, party personal data processor can't request in a way arbitrary all personal data that is not related to the stated goals agreed upon.

Data minimization protects individuals from security from misuse of personal data or unauthorized access to personal data. When data minimization is done, then a collection of personal data is only limited to the required data; there is no need for all other data that is not relevant. This has implications for reducing risk related to violations of personal data protection. Data minimization is also done for guard security individuals in the draft, considering that objective data from existing data processing can be achieved using short and small data.³² Minimizing data is not only done qualitatively to reduce data collection. Still, it can also done qualitatively, for example, using anonymizing personal data.³³

The enforcement principle of human security can also be done as it is the principle of accuracy in processing personal data. That matters Because all processing of personal data must be done according to purpose. When the data does not match the party's data, the processor must directly delete or correct it with accurate data. Data as an object in processing personal data is an important thing when the data is processed, it is not precise, so results from processing are the one that causes it not to achieve the objective of processing personal data. Personal data processors must delete data if it is already relevant to the goal. This is done to protect individuals from all forms of misuse of personal data.

In processing personal data, any personal data is only saved for carrying out objectives from existing processing. No personal data can be saved without a time limit because a time limit works to guard the security of each data individual. However, this is an exception for processed data for interest studies, the data can be saved despite surpassing limitation time.³⁴ Security will still be guaranteed, although processing personal data must be done in a way related to the restriction objective.

³² Privacy International, "Part 3 - Data Protection Principles," A Guide for Policy Engagement on Data Protection (London, August 2018), 41.

³³ Stanislaw Piasecki and Jiahong Chen, "Complying with the GDPR When Vulnerable People Use Smart Devices," *International Data Privacy Law* 12, no. 2 (June 24, 2022): 124–25, <https://doi.org/10.1093/idpl/ipac001>.

³⁴ Rossana Ducato, "Data Protection, Scientific Research, and the Role of Information," *Computer Law & Security Review* 37 (July 2020): 5, <https://doi.org/10.1016/j.clsr.2020.105412>.

Security in processing personal data becomes important, and every data must guarantee integrity and confidentiality. Data confidentiality means that data must be protected and treated as it should be based on the agreement's objective.³⁵ By maintaining the confidentiality of data, it will protect personal data subjects from all threats that exist to them. The threat that arises if personal data is not recorded using encryption is that there could be a leak of their data. Starting from the leak of personal data, it can trigger the emergence of possible misuse of personal data used in action dangerous crime personal data subject.

Human security principles in the context of personal data processing include protecting privacy security and guaranteeing individual freedom regarding their data. This principle exists to protect humans in a digital sector that is developing increasingly rapidly. The processing of personal data must be carried out appropriately by applicable regulations to ensure the security of each data subject. By implementing human security principles in processing personal data, a safe environment will be created for individuals to share their data to achieve specific goals.

Crowdsourcing Personal Data in Human Security Principle

In the current era, this crowdsourcing is commonly used in various applications in various fields.³⁶ Crowdsourcing was first coined by Jeff Howe in 2006, which originated from the words "crowd" and "outsourcing" meaning an organization later will give A task to be determined For members from the crowd.³⁷ In crowdsourcing, many people can contribute online to finish problem.³⁸ In crowdsourcing, individuals contribute to each other to help reach a desired result. Contributors will give various approaches to help the company operate more effectively inside every change policy, science, technology, and sustainable skills.

There are four types of crowdsourcing: crowd-voting from collection voice event mass, crowdsourcing ideas in the form of collecting contributors for input, micro-task crowdsourcing from distribution of a job big become more work small than composed return combined, and solution crowdsourcing from gathering contributors for give a Solution from the problem.³⁹ Crowdsourcing has its characteristics in general: a crowd is

³⁵ Institute of Medicine (US) Committee on Regional Health Data Networks, *Health Data in the Information Age: Use, Disclosure, and Privacy*, ed. Molla S. Donaldson and Kathleen N. Lohr (Washington: National Academies Press (US), 1994).

³⁶ Hui Xu, Yang Wu, and Juho Hamari, "What Determines the Successfulness of a Crowdsourcing Campaign: A Study on the Relationships between Indicators of Trustworthiness, Popularity, and Success," *Journal of Business Research* 139 (February 2022): 484, <https://doi.org/10.1016/j.jbusres.2021.09.032>.

³⁷ Musfiah Saidah, "Crowdsourcing Partisipasi Publik Dalam Proses Menangkal Berita Bohong," *Jurnal Penelitian Komunikasi Dan Opini Publik* 24, no. 1 (July 2020).

³⁸ Mubasher Khalid, Usman Shehzaib, and Muhammad Asif, "A Case of Mobile App Reviews as a Crowdsources," *I.J. Information Engineering and Electronic Business* 7, no. 5 (2015): 39, <https://doi.org/10.5815/ijieeb.2015.05.06>.

³⁹ John Prpić et al., "How to Work a Crowd: Developing Crowd Capital through Crowdsourcing," *Business Horizons* 58, no. 1 (January 2015): 79, <https://doi.org/10.1016/j.bushor.2014.09.005>.

a contributor who has knowledge and skills; contributors complete mandatory tasks; contributors get rewards in a way shaped by material or not; contributors forget entity individual; the prizes will be given must clear the benefits for contributors, assignments given online and participatory, as well use calling open in every variable.

Due to increasingly rapid technological developments, crowdsourcing cannot be separated from humans as contributors. However, what needs to be researched is whether humans as personal data subjects still have their rights protected in crowdsourcing. Protecting data related to privacy is a difficult task and must be done because it concerns the security of humans themselves. Therefore, personal data is proprietary data individual must be stored, cared for, guarded, and protected by confidentiality.⁴⁰

The European Union General Data Protection Regulation (GDPR) defines “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;” Indonesia as a country, the law related to the protection of personal data in Article 1 point 1 of Law Number 27 of 2022 concerning Personal Data Protection has also been provided define personal data as “ data about identified natural persons or can identified in a way separately or combined with information other Good in a way direct nor No direct through system electronic or non-electronic.”

Personal data can be collected and used in the crowdsourcing process for market research, trends analysis, or product development. Collecting personal information via the aforementioned online platform will naturally give rise to worries related to personal data in society. This matter can give rise to risk from misuse of personal data or violation of privacy if not set correctly in its implementation. So, every practice of crowdsourcing must note aspects of security, that is, ensure that personal data is only used for goals that have been agreed upon.

Based on Article 6, GDPR in activity data processing must notice several meaningful things data processing can be done if it fulfills one condition, namely :

a) Consent is a condition where the processing of personal data can happen because permission or agreement exists. The processing of personal data is prohibited except given consent by the personal data subject or permitted by law. There is one permission or agreement for processing personal data based on characteristic volunteers before these data are processed.

⁴⁰ Andriyanto Adhi Nugroho, Atik Winanti, and Surahmad Surahmad, “Personal Data Protection in Indonesia: Legal Perspective,” *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (August 7, 2020): 186, <https://doi.org/10.18415/ijmmu.v7i7.1773>.

- b) Performance of a contract/contractual obligation, i.e., condition a processing of personal data is an implication from contact between individual data processors and personal data subjects. This is a form of agreement between the second split and the taking party steps for data processing.
- c) Legal obligations, that is, condition processing of personal data done to use interest obligation laws regulated by provisions of legislation.
- d) Vital interest, that is, condition data processing is carried out for vital interests of the data subject nor individual others.
- e) Public interest, that is, condition processing done for general interest, which, in its implementation, is authority official and for the public good.
- f) Legitimate interest, condition data processing, is used for clear benefits and legitimate interests, which in matter. This is carried out by the data controller or party when there is only a small risk of violation of the privacy of personal data.

In essence, all data processing for any purpose must be based on the principles stated in regulations regarding personal data protection. The main thing is an agreement between the personal data subject and the personal data processor. Personal data processing can be carried out based on this agreement. Meanwhile, other things that differ from the stated goals agreed upon become things that cannot be done while processing personal data.

In the crowdsourcing process, the processing of personal data will be legitimate if it has fulfilled aspects of principles in processing personal data like legitimacy, fairness, transparency, goal limitations, data minimization, accuracy, limitation storage, integrity, and confidentiality. When the crowdsourcing process is carried out according to criteria, the security of personal data subjects will be guaranteed, so the principle of human security is accomplished. In the crowdsourcing process, it is necessary to confirm contributions made by contributors No cause of loss to them nor other individuals are involved in a way direct in the crowdsourcing process. Loss in a matter this is a threat regarding personal data to those bound in the crowdsourcing approach.

The crowdsourcing process must be done so that volunteers, without coercion, do not break the principle of human security. Contributors have the right to do or not submit personal data to a third-party personal data processor. In terms of this, private data processors carry out a crowdsourcing process. No one will violate human security principles when based on principles processing personal data. During the crowdsourcing process, there is No principle in processing personal data, so it will give rise to loss for individual data subjects, which can have implications for leaking personal data from the contributors. This is contradictory, of course, with principles of human security.

4. Conclusion

Many cases regarding personal data indicated the importance of protecting personal data, which is a right of every individual data subject. In principle, human security personal

data must be covered. For security, man must protected from all possible threats and harm to man. The enforcement principle of human security inside the processing of personal data can be carried out with a guarantee of application validity, fairness and transparency, purpose limitation, data minimization, accuracy, limitations storage, integrity, and confidentiality. That matter is done to protect every personal data subject from all possible threats in the digital era, such as data leaks, which result in the misuse of personal data. In the digital age of personal data processing, often through a crowdsourcing process, the No violate rule principle of human security during No There is consequence losses incurred for contributor nor individual other. So, the crowdsourcing approach must emphasize principles of processing personal data to ensure protection and security for every individual.

Refrences

- Alafaa, Princess. "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World." *SSRN Electronic Journal*, 2022. <https://doi.org/10.2139/ssrn.4005750>.
- Asolund, Bo, and Romeo Reyes. "Human Security, Human Development, and The Millenium Development Goals" *Indonesian Journal of International Law* 1, no. 1 (August 12, 2021). <https://doi.org/10.17304/ijil.vol1.1.168>.
- BBC News. "TikTok sued for billions over use of children's data." April 21, 2021, sec. Technology. <https://www.bbc.com/news/technology-56815480>.
- Bofa, Maya, Darmawan Wawan Budi, and Arifin Sudirman. "Data Rights di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook dalam Pemilihan Presiden Amerika Serikat 2016." *Hasanuddin Journal of International Affairs* 2, no. 2 (November 27, 2022): 144–59. <https://doi.org/10.31947/hjirs.v2i2.22686>.
- Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, March 17, 2018, sec. News. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- "Can We Use Data for Another Purpose?" Accessed December 3, 2023. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en.
- Candra, Darang S, and Broto Wardoyo. "Implementing Human Security Measures in the Cyberspace: Navigating through the Institutional and Regulatory Disarray," n.d.
- Clifford, Damian, and Jef Ausloos. "Data Protection and the Role of Fairness." *CiTiP Working Paper 29/2017*, August 2017.

- "Complete Chronology of 91 Million Tokopedia Accounts Leaked and Sold." Accessed December 12, 2023. <https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual>.
- "Data Protection and Privacy Laws | Identification for Development." Accessed December 3, 2023. <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>.
- Ducato, Rossana. "Data Protection, Scientific Research, and the Role of Information." *Computer Law & Security Review* 37 (July 2020): 105412. <https://doi.org/10.1016/j.clsr.2020.105412>.
- Elison, Larry M. "Right of Privacy." *Montana Law Review* 48, no. 1 (January 1987).
- Estrada, Paola. "Global Data Privacy Practices and the Importance of Privacy Awareness in Today's Virtual Realm." *SSRN Electronic Journal*, 2022. <https://doi.org/10.2139/ssrn.4118695>.
- Forgó, Nikolaus, Stefanie Händel, and Benjamin Schütze. "The Principle of Purpose Limitation and Big Data." In *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation*. Singapore: Springer, 2017.
- Goldhill, Olivia. "A 'big data' firm sells Cambridge Analytica's methods to global politicians, documents show." *Quartz*, August 14, 2019. <https://qz.com/1666776/data-firm-idea-uses-cambridge-analytica-methods-to-target-voters>.
- Haubert, Brandon. "Roblox Is Stealing Your Kids Biometric Data." *wh Law*, February 15, 2022. <https://whlawoffices.com/blog/roblox-is-stealing-your-kids-biometric-data/>.
- Healey, Robert. "The Principle of Lawfulness, Fairness, and Transparency." *Formiti*, October 23, 2023. <https://formiti.com/data-privacy-the-principle-of-lawfulness-fairness-and-transparency/>.
- Institute of Medicine (US) Committee on Regional Health Data Networks. *Health Data in the Information Age: Use, Disclosure, and Privacy*. Edited by Molla S. Donaldson and Kathleen N. Lohr. Washington: National Academies Press (US), 1994.
- Khalid, Mubasher, Usman Shehzaib, and Muhammad Asif. "A Case of Mobile App Reviews as a Crowdsourcing." *I.J. Information Engineering and Electronic Business* 7, no. 5 (2015): 39. <https://doi.org/10.5815/ijieeb.2015.05.06>.
- Kharisma, Dona Budi. "Urgency of Financial Technology (Fintech) Laws in Indonesia", *International Journal of Law and Management*, 63(3), 2021, pp. 320–331. Available at: <https://www.emerald.com/insight/content/doi/10.1108/IJLMA-08-2020-0233/full/html>
- Kharisma, Dona Budi. "Membangun Kerangka Pengaturan Startup Di Indonesia", *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, [S.l.], v. 10, n. 3, p. 431-445, dec. 2021. ISSN 2580-2364. doi: <http://dx.doi.org/10.33331/rechtsvinding.v10i3.766>
- Kharisma, Dona Budi and Hunaifa, Alfiya. "Comparative study of disgorgement and disgorgement fund regulations in Indonesia, the USA and the UK", *Journal of Financial Crime*, 30(3) 2022, pp. 635–649. Available at: <https://doi.org/10.1108/JFC-01-2022-0022>.
- Makarim, Edmon. *Kompilasi Hukum Telematika*. Jakarta: PT. Raja Grafindo Perkasa, 2003.
- . *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*. Jakarta: Rajawali Pers, 2010.

- Nugroho, Andriyanto Adhi, Atik Winanti, and Surahmad Surahmad. "Personal Data Protection in Indonesia: Legal Perspective." *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (August 7, 2020): 183. <https://doi.org/10.18415/ijmmu.v7i7.1773>.
- Pelteret, Marc, and Jacques Ophoff. "A Review of Information Privacy and Its Importance to Consumers and Organizations." *Informing Science: The International Journal of an Emerging Transdiscipline* 19 (2016). <https://doi.org/10.28945/3573>.
- Piasecki, Stanislaw, and Jiahong Chen. "Complying with the GDPR When Vulnerable People Use Smart Devices." *International Data Privacy Law* 12, no. 2 (June 24, 2022): 113–31. <https://doi.org/10.1093/idpl/ipac001>.
- Privacy International. "Part 3 - Data Protection Principles." A Guide for Policy Engagement on Data Protection. London, August 2018.
- Prpić, John, Prashant P. Shukla, Jan H. Kietzmann, and Ian P. McCarthy. "How to Work a Crowd: Developing Crowd Capital through Crowdsourcing." *Business Horizons* 58, no. 1 (January 2015): 77–85. <https://doi.org/10.1016/j.bushor.2014.09.005>.
- Raihan, Muhammad. "Perlindungan Data Diri Konsumen dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)". *Jurnal Inovasi Penelitian* 3, no. 10 (March 2023).
- Ray, Siladitya. "Class Action Lawsuit Alleges TikTok 'Collected Data From Minors, Sent It To Servers In China.'" *Forbes*. Accessed November 28, 2023. <https://www.forbes.com/sites/siladityaray/2020/08/05/class-action-lawsuit-alleges-tiktok-collected-data-from-minors-sent-it-to-servers-in-china/>.
- Saidah, Musfiah. "Crowdsourcing Partisipasi Publik Dalam Proses Menangkal Berita Bohong" *Jurnal Penelitian Komunikasi Dan Opini Publik* 24, no. 1 (July 2020).
- Statista. "Internet and Social Media Users in the World 2023." Accessed November 13, 2023. <https://www.statista.com/statistics/617136/digital-population-worldwide/>.
- Supriyadi, Daniar. "The Regulation of Personal and Non-Personal Data in the Context of Big Data." *Journal of Human Rights, Culture and Legal System* 3, no. 1 (February 14, 2023): 33–69. <https://doi.org/10.53955/jhcls.v3i1.71>.
- Tadjbakhsh, Shahrbanou, and Anuradha Chenoy. *Human Security: Concepts and Implications*. 1st ed. London: Routledge, 2007.
- Thaorey, Payal. "Legal Intropection Towards the Development of Right to Privacy as Fundamental Right in India" *Indonesia Law Review*. Vol. 11, no. 3 (2021).
- United Nations. *Human Security Handbook*, 2016.
- Verhenneman, Griet. *The Patient, Data Protection and Changing Healthcare Models: The Impact of e-Health on Informed Consent, Anonymisation and Purpose Limitation*. KU Leuven Centre for IT & IP Law Series. Cambridge: Intersentia, 2021.
- Xu, Hui, Yang Wu, and Juho Hamari. "What Determines the Successfulness of a Crowdsourcing Campaign: A Study on the Relationships between Indicators of Trustworthiness, Popularity, and Success." *Journal of Business Research* 139 (February 2022): 484–95. <https://doi.org/10.1016/j.jbusres.2021.09.032>.