INTERNATIONAL JOURNAL OF JUDICIAL LAW

Facial Recognition in Photo Marketplace: Legal Analysis of FotoYu under Indonesia's ITE and Personal Data Protection Law

I Gusti Ayu Nadya Candra Pramitha [1*], Dr. I Nyoman Bagiastra [2]
[1-3] Faculty of Law, Udayana University, Indonesia

* Corresponding Author: **I Gusti Ayu Nadya Candra Pramitha**

Article Info

ISSN (online): 2583-6536
Volume: 04
Issue: 04
July - August 2025
Received: 29-05-2025
Accepted: 20-06-2025
Published: 21-07-2025
Page No: 86-91

Abstract
The rapid development of photo applications based on artificial intelligence (AI) raises urgent legal questions related to user privacy, data protection, and digital consent. FotoYu, an Indonesia-based platform that enables users to purchase candid public photos of themselves through facial recognition technology, serves as a unique case study to evaluate compliance with the national legal framework. This article analyzes FotoYu's operational model based on Law Number 11 of 2008 concerning Electronic Information and Transactions (EIT Law) and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The main legal issues raised include the classification of biometric data, the legal basis for data processing, and the limitations of using implied consent in public spaces.
Using a normative-juridical approach, this study critiques FotoYu's reliance on facial recognition technology (through AI RoboYu) in the absence of a clear and explicit consent mechanism. A comparative perspective from the GDPR and the practice of facial recognition use in European Union jurisdictions provides normative insights for regulating similar technologies. This analysis concludes that although FotoYu's operations fall within a legal grey area, stricter law enforcement and clearer regulatory guidelines are required to protect user rights and prevent misuse. Recommendations include stricter obligations for data controllers, explicit consent protocols, and specific sectoral regulations for AI-based platforms.

DOI: https://doi.org/10.54660/IJJL.2025.4.4.86-91

Keywords: Facial Recognition Technology, FotoYu, Indonesian EIT Law, Personal Data Protection, Digital Consent

Introduction

In the digital era, the rapid advancement of artificial intelligence (AI) and data-driven technologies has significantly transformed the way individuals interact with digital platforms. The integration of facial recognition technology into everyday mobile applications once limited to the domains of security and law enforcement, has now expanded into consumer services, including photography, social media, and e-commerce. This evolution has not only generated new business models but also reshaped the meaning of privacy, identity, and consent in the digital public sphere.

Indonesia, as one of the largest digital markets in Southeast Asia, is currently experiencing a surge of innovation across various technology-based platforms. Among these innovations is FotoYu, a mobile application that enables users to search for and purchase candid photographs of themselves taken in public spaces. This functionality is made possible by a proprietary facial recognition engine named "RoboYu," which analyzes user-uploaded selfies and matches them against images stored in the system. Although FotoYu is marketed as a tool for discovering spontaneous moments or reliving forgotten memories, its technological operation involves the collection and processing of sophisticated biometric data in ways that are largely opaque. Unlike traditional data collection, wherein users voluntarily submit personal information, FotoYu's system gathers facial data without the knowledge or explicit consent of the data subjects, often through third-party photographers operating in public areas.

Such an operational model raises urgent legal and ethical concerns, especially within the context of personal data protectio.

The concept of consent, long regarded as the cornerstone of privacy protection, becomes ambiguous when individuals are unaware that their facial data has been captured, processed, or even commercialized. This gives rise to a critical legal question: Can a platform lawfully process biometric data obtained from public spaces without prior consent especially when such data is subsequently monetized?

Indonesia's legal response to this challenge is reflected in two principal instruments: Law Number 11 of 2008 concerning Electronic Information and Transactions (EIT Law), and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law constitutes Indonesia's first comprehensive regulation governing personal data protection, including provisions on data controllers, explicit consent, and the rights of data subjects. The law explicitly classifies biometric data, including facial features, as specific personal data requiring a higher level of protection. Under these provisions, platforms such as FotoYu that collect and determine the purpose of data usage are designated as data controllers and are therefore subject to a range of legal obligations, including transparency, data security, lawful bases for processing, and facilitation of user rights.

However, the implementation of these legal requirements remains uncertain, particularly in relation to AI-based platforms operating in non-traditional ways. FotoYu, for instance, does not provide notice to individuals whose images are being processed, nor does it offer mechanisms for granting or refusing consent, submitting deletion requests, or objecting to data processing. Such practices appear inconsistent with the principles enshrined in the PDP Law and may indicate gaps in regulatory enforcement in Indonesia. Furthermore, when compared with international standards such as the European Union's General Data Protection Regulation (GDPR), Indonesia's legal framework appears not yet fully equipped to address the complexities of the relationship between innovation and privacy rights within the context of biometric surveillance.

Globally, facial recognition technology has sparked significant controversy across both public and private sectors. While certain governments and corporations have embraced this technology for its efficiency and automation capabilities, others particularly in Europe and North America—have voiced strong opposition due to its potential misuse in mass surveillance, discrimination, and the erosion of individual freedoms. Regulatory authorities in the European Union have established clear standards regarding biometric data, including requirements for explicit consent, data protection impact assessments, and accountability obligations for data controllers. These international responses underscore the importance for Indonesia to critically assess whether its current legal framework and institutional infrastructure are adequate to regulate AI-based platforms that operate across the blurred boundaries of private space, public visibility, and commercial interest.

Against this backdrop, the present study focuses on analyzing the legal responsibility of platforms such as FotoYu as data controllers under the Personal Data Protection Law (PDP Law), while also comparing these responsibilities with global standards for data and privacy protection. The objective is to assess whether FotoYu's business practices align with its legal obligations concerning biometric data processing, and to explore necessary legal reforms or regulatory strategies to ensure compliance and the protection of individual rights within Indonesia's rapidly evolving digital landscape.

Problem Formulation

1. Does the collection and use of facial data by FotoYu constitute processing of personal data under Indonesian Law?
2. What are the legal responsibilities of platforms such as FotoYu as data controllers under the PDP Law, and how these responsibilities compare with global standards?

Purpose

This study aims to critically examine the legal implications of the use of facial recognition technology by FotoYu within the context of Indonesia's digital regulatory framework. As an artificial intelligence (AI)-based platform that enables users to search for and purchase photographs through facial image matching without obtaining prior consent, FotoYu presents a relevant case study to assess the extent to which Indonesia's data protection laws can accommodate the challenges posed by such emerging technologies. Specifically, this research seeks to analyze whether FotoYu's practices of collecting and processing biometric data, particularly facial features constitute lawful conduct under the provisions of the Electronic Information and Transactions Law (EIT Law) and the Personal Data Protection Law (PDP Law). Furthermore, the study will evaluate whether the platform's consent mechanism or lack thereof complies with the legal standards governing the processing of sensitive personal data.

In its analysis, this research will explore FotoYu's legal obligations as both an electronic system operator and a data controller, with particular emphasis on transparency, security, and accountability in data governance. To broaden the analytical framework, this study also refers to the European Union's General Data Protection Regulation (GDPR) to highlight normative gaps and identify best practices that may serve as regulatory benchmarks.

Ultimately, the study seeks to provide policy recommendations aimed at strengthening Indonesia's legal and ethical framework in response to AI-based data collection practices within the digital public sphere.

Discussion

A. The Colletion and Use of Facial Data by FotoYu Constitute Processing of Personal Data under Indonesian Law

The use of facial recognition technology by the FotoYu application in providing automated facial matching services and photo sales raises significant legal concerns, particularly within the framework of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and its implementing regulations. According to the PDP Law, personal data is comprehensively defined as any information that may identify an individual, either directly or indirectly. This term encompasses biometric data, including face data which is categorized as a specific (sensitive) type of personal data due to its unique characteristics and its inherent ability to directly

identify an individual [1].

FotoYu's facial matching feature, powered by the RoboYu algorithm, processes unique facial features captured from images taken in public spaces and matches them against selfies uploaded by users. Since this method relies on a person's likeness to verify their identity, it surely constitutes the processing of biometric data, which is defined as specific (sensitive) personal information under Article 4, paragraph (2) of the Personal Data Protection Law (PDP Law). In addition, the PDP Law defines "processing" as a series of operations that include gathering, organising, storing, adapting, modifying, retrieval, use, disclosure, dissemination, and deletion or destruction of personal data (Article 16, paragraph 1) among others [2] According to the applicable legal laws, FotoYu's activities—which include collecting, analysing, matching, and selling face pictures—clearly comprise the processing of personal data.

The compliance of FotoYu's face recognition technology with the Personal Data Protection Law (PDP Law) is crucial to its legitimacy. In order to handle some types of personal data, such as biometric data, the PDP Law states in Article 20 that the data subject must provide their express and informed consent before any processing may take place [3]. However, FotoYu does not obtain such consent from individuals before their images are captured, their facial features processed, or their likeness monetized. In fact, notification is only provided to individuals after a successful match is made and the user is notified via the application a practice that violates both the textual and substantive requirements for consent under the PDP Law. Consent must be explicit, voluntary, specific, and informed criteria that are not satisfied under FotoYu's current operational model.

As a data controller, FotoYu is subject to the legal obligations set forth in Articles 21 to 39 of the Personal Data Protection Law (PDP Law). These obligations include providing clear notice to data subjects, ensuring the security of personal data, guaranteeing that data processing is conducted in a proportional and relevant manner, and offering data subjects access to rectify or delete their data [4]. However, FotoYu's current operational model fails to provide meaningful transparency or user control. Individuals whose images are processed have no prior knowledge of the processing, are unable to opt out, and lack any clear mechanism to request data erasure or object to the processing. Such practices are in direct conflict with the fundamental principles of fairness, transparency, accountability, and data minimization.

Furthermore, Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law) reinforces the provisions of the Personal Data Protection Law (PDP Law) by mandating that any use of personal data within an electronic system must be preceded by the consent of the data subject. Article 26 paragraph (1) of the EIT Law affirms that user consent is an absolute requirement prior to the electronic use of personal data. Accordingly, FotoYu's business model potentially violates both the PDP Law and the EIT Law particularly in cases where users suffer reputational, psychological, or economic harm as a result of their facial images being used without authorization.

Indonesia's data protection framework is relatively nascent, and while the Personal Data Protection Law (PDP Law) incorporates aspects of international regulations like the European Union's General Data Protection Regulation (GDPR), the lack of comprehensive implementing regulations and robust oversight mechanisms has constrained its enforcement. In contrast, the GDPR mandates that data controllers handling biometric data for purposes like as profiling or tracking do a DPIA to foresee and alleviate risks to individual rights [5] Similarly, under the California Consumer Privacy Act (CCPA), users are granted specific rights, including the right to opt out of the sale of their personal data. These international standards highlight the importance of prior consent, risk assessment, and individual control, elements that are still insufficiently present in the operational environment of facial recognition technology in Indonesia.

From an ethical perspective, FotoYu's practices raise serious concerns regarding the erosion of personal autonomy. While individuals photographed in public spaces may not reasonably expect absolute privacy, the systematic, automated, and commercial exploitation of their images without their knowledge transforms mere presence in public into a commodified form of surveillance. This practice not only undermines digital trust but also infringes upon the constitutional right to privacy as enshrined in Article 28G of the 1945 Constitution of the Republic of Indonesia [6]. The absence of meaningful and contextual consent. especially when data captured in public is sold for private gain reflects a profound disregard for personal dignity and individual control over one's digital identity.

In conclusion, The processing of biometric facial data by FotoYu, including its collection and utilization clearly fall within the scope of personal data processing under Indonesian law. Both the Personal Data Protection Law (PDP Law) and the Electronic Information and Transactions Law (EIT Law) require explicit, informed, and prior consent, the fulfillment of data subject rights, and the implementation of robust security mechanisms. FotoYu's failure to comply with these legal obligations presents serious legal and ethical risks. Without substantial changes to its operational model particularly regarding consent mechanisms, user transparency, and regulatory compliance FotoYu's facial recognition service stands in direct conflict with Indonesia's personal data protection regime and broader principles of human rights.

[1] Mardisontori M. Legal Review of Personal Data Regulations In The Personal Data Protection Law. In: Proceedings of the First International Cyber Law Conference (ICL-C 2023). Jakarta: EAI; 2025.

[2] Lestari E, Rasji R. Legal Study on Personal Data Protection Based on Indonesian Legislation. Awang Long Law Rev. 2024 May;6(2):471–477

[3] Salsabila SS. Personal Data Protection Policy in Law Number 27 of 2022 in Facing the Digital Era in Indonesia. Edusight Int J Multidiscip Stud. 2024 Jun;1(2):1-10

[4] Shahrullah RS, Park J, Irwansyah I. Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. Hasanuddin Law Rev. 2024 Apr;10(1):1–20

[5] Pramudya AHP, Hasibuan FY, Sitompul Z. Legal Protection in the Processing and Exchange of Personal Data by Financial Technology Companies. Asian J Soc Humanit. 2024;3(2):247–260.

[6] Sa'adah BLN, Sukarni S, Dewantara R. Establishing a Personal Data Protection Agency for E-Commerce in Indonesia: Legal Framework and Implementation Challenges. Invest J Sharia Econ Law. 2024 Dec;4(2):292–316.

B. Legal Responsibilities of Platforms Such as Fotoyu As Data Controllers Under the PDP Law, and how These Responsibilities Compare with Global Standards.

Under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), platforms such as FotoYu which collect, process, and store personal data are legally classified as data controllers. As defined in Article 1 point 4 of the PDP Law, a data controller is any party that determines the purposes and exercises control over the processing of personal data. FotoYu, which collects and processes biometric data in the form of users' facial features categorized as specific (sensitive) personal data under Article 4 paragraph (2) clearly falls within this definition. The operations of the application, including the collection of user selfies, automated facial matching via the RoboYu technology, and the offering of matched images for purchase, all constitute forms of processing, as defined under Article 1 point 5 of the PDP Law. This includes activities such as collection, recording, storage, use, display, transmission, and deletion of data.

As a data controller, FotoYu bears specific legal obligations as set forth in Chapter VI of the PDP Law. These include obtaining valid and explicit consent (Articles 20–22), ensuring transparency in data processing (Article 23), guaranteeing the security and confidentiality of personal data (Article 39), and fulfilling the rights of data subjects including the rights to access, rectification, erasure, and objection (Articles 5–13). These obligations are generally aligned with global data protection standards, such as the European Union's General Data Protection Regulation (GDPR), although the PDP Law also reflects Indonesia's unique regulatory context. Particularly for specific personal data such as biometric information, the PDP Law mandates that explicit consent must be obtained consciously, freely, and prior to any processing activity. In the case of FotoYu, there is no evidence that such consent has been obtained from individuals whose facial data was collected in public spaces by third-party photographers and subsequently matched through the application. Even if end-users provide consent by uploading their own selfies, the facial data of other individuals (non-users), who are unaware that they were photographed, is also processed often without any notification or opportunity to provide consent. The absence of prior notification and consent potentially places FotoYu in breach of its legal obligations under the PDP Law.

Data subjects must provide clear, unambiguous, and informed permission before FotoYu may collect and handle their personal data [7]. Furthermore, the platform must use suitable security technologies, conduct frequent audits, and employ encryption to safeguard personal data from misuse, unauthorised access, data breaches, and improper implementation of organisational and technological policies. Adopting internal procedures to guarantee legal compliance and maintaining open communication with data subjects about data collection, use, storage, and sharing are all essential components of transparency, which is a fundamental requirement in and of itself [8]. Additionally, FotoYu has to make sure that people may access, correct, delete, and limit processing of personal data. Any delay in reporting the occurrence and cooperating with the appropriate authorities might lead to legal ramifications in the case of a breach or hack, therefore the organisation must act swiftly. The PDP Law also mandates both preventive measures, such as securing data systems, and remedial actions, including administrative or criminal sanctions, to ensure legal enforcement. Although the PDP Law mandates the establishment of an independent supervisory authority, this body has not yet become fully operational, resulting in uncertainty regarding oversight and enforcement mechanisms [9].

There are several striking parallels and differences when compared to international data protection laws, such as the General Data Protection Regulation (GDPR). The concepts of lawfulness, equity, openness, purpose restriction, data minimisation, precision, storage limitation, and secrecy are central to both systems of law. In addition to requiring permission, they provide data subjects extensive rights, such as the ability to access, correct, delete, and object to data processing. Data controllers are required to establish strong security measures to safeguard personal data under the GDPR, just as they are under Indonesia's PDP Law. But in a number of important respects, the GDPR goes beyond. Facial recognition in public places is one example of a high-risk processing activity that must undergo a Data Protection Impact Assessment (DPIA). Furthermore, in some high-risk situations, it mandates the appointment of a Data Protection Officer (DPO) (Article 37), a need that is currently absent from Indonesian law.

Another crucial divergence lies in the area of enforcement. The GDPR is backed by well-established supervisory authorities across EU member states, equipped with strong investigative powers, including the authority to impose substantial administrative fines (up to 4% of global annual turnover). In contrast, Indonesia continues to face challenges in operationalizing the independent supervisory authority mandated by the PDP Law. Although the law provides for administrative, civil, and criminal sanctions, institutional limitations weaken enforcement, accountability, and legal recourse for affected individuals. Enforcement delays are particularly evident in sensitive sectors such as banking, where data protection violations have already begun to emerge [10].

From a broader perspective, International privacy standards, including the OECD Privacy Guidelines and the APEC Privacy Framework, underscore the importance of user autonomy in personal data processing. purpose limitation, data minimization, and informed consent. FotoYu's business model, which involves the collection of facial data without prior consent, fails to provide notice to affected individuals and does not offer meaningful opt-out or data deletion mechanisms. As such, it falls short of these international standards. Ethical concerns surrounding biometric surveillance also raise additional issues, including the risk of function creep, the commodification of identity, and the erosion of individual control over one's digital self. In a democratic legal system, data controllers are expected not

[7] Jannah M, Amboro FYP, Shahrullah RS. Personal data protection in telemedicine: comparison of Indonesian and European Union law. J Law Policy Transform. 2023 Dec;8(2):145–163

[8] Hartanto S, Putri PP. Protection of notaries as controllers and processors of personal data of litigants. Jurnal Ius Constituendum. 2025 Jun;10(2):184–199

[9] Kurdi K, Cahyono J. Perlindungan data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. Juncto J Ilm Huk. 2024;6(2):330–339

[10] Kholis IM. Perlindungan data pribadi dan keamanan siber di sektor perbankan: studi kritis atas penerapan UU PDP dan UU ITE di Indonesia. STAATSRECHT: Jurnal Hukum Kenegaraan dan Politik Islam. 2024 Des;4(2):275–300

only to comply with minimum legal requirements but also to uphold proactive ethical responsibilities.

Moreover, several platforms outside Indonesia, such as SpotMyPic (United States), Revopic (Netherlands), TurtlePic (Germany), and FaceFindr (Australia) demonstrate that facial recognition services can operate while adhering to strict data protection standards. These platforms, often used in public events such as races or weddings, only allow users to search for and purchase photos after uploading a selfie or entering an identifier (e.g., race bib number). They use encrypted facial data, watermarked image previews, and avoid public display of images without consent. Some even offer private modes, allowing images to remain hidden until user verification is complete. These international practices reflect a higher standard of transparency and accountability a standard that, in its current form, FotoYu has yet to meet [11].

Conclusion

Based on the analysis conducted by the author regarding the issues previously discussed, it can be concluded that:

1. The collection and use of facial data by FotoYu clearly falls within the definition of personal data processing as stipulated under the Indonesian Personal Data Protection Law (PDP Law). The application collects and analyzes biometric identifiers classified as specific (sensitive) personal data without obtaining the explicit and informed consent of the data subjects. FotoYu's operational model, which matches users with candid photographs using AI-powered facial recognition technology without direct communication or prior notification, constitutes processing as defined in Article 1 point (5) and Article 4 paragraph (2) of the PDP Law. This raises significant concerns regarding the legality, transparency, and fairness of data management, particularly since the data is collected passively in public spaces.
2. As a data controller, FotoYu bears legal obligations in accordance with the provisions of the Personal Data Protection Law (PDP Law) to uphold the principles of informed consent, data security, transparency, and the protection of data subject rights. However, the platform's current practices fall short of these standards, particularly in obtaining valid consent and granting users meaningful control. When compared to jurisdictions governed by the General Data Protection Regulation (GDPR) in the European Union, the Act on the Protection of Personal Information (APPI) in Japan, or the Personal Information Protection Act (PIPA) in South Korea, Indonesia's enforcement mechanisms and accountability frameworks remain relatively underdeveloped. Many international platforms offering similar photo-matching services have implemented stronger safeguards such as private modes, user-triggered matching, data encryption, and consent-based image display all of which are currently absent from FotoYu's operational system.

Suggestion

1. The Government of Indonesia particularly the forthcoming data protection authority must promptly issue specific guidelines governing the use of facial recognition technology in both public and commercial contexts. Platforms such as FotoYu should be required to adopt a consent-first model, ensuring that data subjects are fully aware of data collection activities and are provided with clear opt-in/opt-out mechanisms. Additionally, transparency obligations should be enforced, including the publication of privacy notices and the provision of individual rights to access and request the deletion of their personal data.
2. FotoYu must undertake substantial reforms to its operational model and legal compliance framework by aligning with international best practices, particularly as set forth in the General Data Protection Regulation (GDPR). Indonesian regulators must also prioritize institutional capacity-building to ensure the effective enforcement of the Personal Data Protection Act. This includes the establishment of a strong and independent supervisory authority, public education on biometric privacy, and the requirement for platforms to conduct Data Protection Impact Assessments (DPIAs) prior to implementing AI-based data processing systems. Furthermore, all platforms must ensure the ethical use of facial recognition technologies, striking a balance between innovation and the protection of individual rights and human dignity.

References

1. Mardisontori M. Legal review of personal data regulations in the Personal Data Protection Law. In: Proceedings of the First International Cyber Law Conference (ICL-C 2023). Jakarta: EAI; 2025.
2. Lestari E, Rasji R. Legal study on personal data protection based on Indonesian legislation. Awang Long Law Rev. 2024 May;6(2).
3. Salsabila SS. Personal data protection policy in Law Number 27 of 2022 in facing the digital era in Indonesia. Edusight Int J Multidiscip Stud. 2024 Jun;1(2).
4. Shahrullah RS, Park J, Irwansyah I. Examining personal data protection law of Indonesia and South Korea: the privacy rights fulfilment. Hasanuddin Law Rev. 2024 Apr.
5. Pramudya AHP, Hasibuan FY, Sitompul Z. Legal protection in the processing and exchange of personal data by financial technology companies. Asian J Soc Humanit. 2024;3(2).
6. Sa'adah BLN, Sukarni S, Dewantara R. Establishing a personal data protection agency for e-commerce in Indonesia: legal framework and implementation challenges. Invest J Sharia Econ Law. 2024 Dec;4(2).
7. Jannah M, Amboro FYP, Shahrullah RS. Personal data protection in telemedicine: comparison of Indonesian and European Union law. J Law Policy Transform. 2023 Dec;8(2).
8. Hartanto S, Putri PP. Protection of notaries as controllers and processors of personal data of litigants. Jurnal Ius Constituendum. 2025 Jun;10(2).
9. Kurdi K, Cahyono J. Perlindungan data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. Juncto J Ilm Huk. 2024;6(2).
10. Kholis IM. Perlindungan data pribadi dan keamanan siber di sektor perbankan: studi kritis atas penerapan UU PDP dan UU ITE di Indonesia. STAATSRECHT J Huk Kenegaraan Polit Islam. 2024 Dec;4(2).

[11] Ravinka NA, Widiatedja IGNP. What should Indonesia learn from rights to data privacy under the GDPR? Kertha Semaya. 2022;10(3):583–595.

11. Ravinka NA, Widiatedja IGNP. What should Indonesia learn from rights to data privacy under the GDPR? Kertha Semaya. 2022;10(3).
12. European Union. General Data Protection Regulation (GDPR).
13. Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.
14. Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.