Volume 4, No. 1 January 2025 - (203-217)
p-ISSN 2980-4868 | e-ISSN 2980-4841
https://ajesh.ph/index.php/gp

Wearable Technology in the Perspective of Personal Data Protection Law: A Comparative Study Between Indonesia and the European Union

Erika Leony[1*], Tjhong Sendrawan[2]
Universitas Indonesia, Indonesia
Emails: erikaleonyy26@gmail.com

ABSTRACT
Wearable Technology is a device that functions by recording and collecting various user data, including personal activities as well as physiological and environmental data. This technology allows users to independently monitor and manage their health through the information provided. However, behind its benefits, there are risks related to data privacy and security, especially since health information is sensitive and confidential. Therefore, this study aims to analyze the protection of personal data in the use of wearable technology, highlighting the importance of adequate regulation. This research uses a normative method with a statutory approach to examine the personal data protection regulations applicable in Indonesia, particularly in the context of the Personal Data Protection Law (PDP Law). In addition, this research conducts a comparative study with data protection regulations in the European Union (EU) to identify the strengths and challenges in the implementation of data protection policies in Indonesia. The results show that although UU PDP has provided a legal foundation for personal data protection, there are still several aspects that need to be strengthened in order to accommodate increasingly complex technological developments. The implications of this research highlight the need to increase user awareness and strengthen law enforcement mechanisms to ensure more effective data protection in the use of wearable technology.

Keywords: Wearable Technology, Personal Data Protection, Digital Security and Privacy, Personal Data Protection Law, European Union Data Protection Regulation.

INTRODUCTION

Technology in the current era continues to evolve with the drive to improve the latest services and the high demand from consumers for digital advancements. One of the versatile technologies that are widely used by individuals today is "wearable technology" (Çiçek, 2015). In recent years, wearable technology has developed rapidly, even becoming an important part of everyday life (Lee et al., 2016). Devices such as smartwatches, fitness trackers, and wearable health monitors are increasingly popular due to their ability to monitor health, physical activity, and various aspects of their users' lives in real-time. Aside from its ability to monitor the health

of its users, these devices can serve to increase productivity, as well as simplify the lives of its users in accessing information.

The term wearables, wearable devices, or wearable technology refers to small electronic, mobile, or computer devices with wireless communication capabilities incorporated into gadgets, accessories, or clothing, which can be used on the human body or even invasive versions such as microchips or smart tattoos (Ometov et al., 2021). This technology is different from smartphones or tablets, with the added value of various monitoring and scanning features, including biofeedback or other sensory physiological functions such as those related to biometry. These devices are designed to be comfortable and portable to offer hands-free access to electronic devices. Examples of current wearable technology are conventional sports trackers, smartwatches, body cameras, heart rate meters, and smart glasses, but it is predicted that the next generation of wearable devices will also involve augmented, virtual, mixed, and augmented-reality devices, various smart clothing, and wearable industrial equipment (Aroganam et al., 2019).

Besides the services offered, wearable technology also records and collects various data such as personal activity and physiological and environmental data of its users. This data is provided so that users can monitor their own health with a lot of personal information provided, such as heart rate, blood pressure, blood sugar, cholesterol, weight, personal activity range, habits, and more (Vijayan et al., 2021). Wearables work by collecting numerical data at specific periods, which is carried out and evolves over time to form a temporal stream data set. With so much detailed personal data collected by these devices, they are certainly very useful for their users.

Despite the benefits of wearable technology, such as easier data tracking and better health management, there are potential risks associated with data privacy and security (Sivakumar et al., 2024). It is important to emphasize the importance of privacy in wearable technology because personal health-related data is highly sensitive and confidential. Unauthorized access or misuse of this data has led to privacy concerns that are certainly not simple.

According to the results of an investigation conducted in 2018, it shows that most apps do not follow the rule of law, and there is a fact that the collected user data sets have been sent to third parties who have a partner relationship with the app in question. Hackers can directly obtain user privacy data, so there is a possible risk of personal data leakage, such as exposure to health problems, living habits, and scope of activities (Aswathy & Tyagi, 2022). Privacy issues are not the only major challenge in the concept of wearable technology, besides the ability of wearable devices to sense, capture and store sensitive information about users and their environment, these devices can also do so continuously and secretly.

Therefore, it is very important to realize the protection of user data privacy without affecting data collection on wearable services. In Indonesia, the availability of regulations regarding the protection of personal data is tiered. Prior to the enactment of Law No. 27 of 2022

on Personal Data Protection (UU PDP), regulations regarding the protection of personal data in Indonesia were scattered in several laws and regulations and more rigidly regulated in Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (PP No. 71 of 2019) and Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016 on the Protection of Personal Data in Electronic Systems (Permenkominfo No. 20 of 2016), while at the Law level, this has not been explicitly regulated.

The issuance and enactment of the PDP Law provides legal certainty regarding personal data for the people of Indonesia. The PDP Law defines personal data as data relating to an individual who can be identified either individually or first needs to be combined directly or indirectly with other information through electronic or non-electronic systems (Sahib et al., 2023). Meanwhile, the protection of personal data of data subjects is all activities aimed at protecting user data during a series of personal data processing in order to achieve the constitutional rights of each personal data subject.

According to the PDP Law, personal data can be classified into two types: specific personal data and general personal data (Suari & Sarjana, 2023). Specific personal data includes health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and/or other data in accordance with the provisions of laws and regulations. Meanwhile, general personal data includes full name, gender, religion, marital status, and/or Personal Data that is combined to identify a person. Thus, the data collected by the wearable device is specific personal data, where any processing activity on the data can have a greater impact on the possibility of discrimination or harm to the data subject. The processing activities on personal data include the acquisition and collection, processing and analysis, storage, correction and updating, displaying, publishing, transferring, disseminating, disclosing, and deletion of data. Data processing activities shall be carried out in compliance with the principles of data protection and shall first obtain the express consent of the data subject, fulfillment of the controller's legal obligations, and protection of the vital interests of the data subject.

Data processing activities are the responsibility of the controller, so if there is a breach in the processing activities, the PDP Law provides penalties in the form of administrative sanctions for the controller. Based on these provisions, it can be concluded that every activity of collecting and processing personal data must be based on the consent of the data owner himself. The data owner concerned has the right to know the process of use, storage of data and if the data is shared by the Personal Data Controller. This is important, because every personal data can only be used for the purposes and purposes that have been previously agreed by the data owner. In addition, the PDP Law also provides sanctions, namely administrative and criminal sanctions, for parties who violate the provisions of this legislation.

When looking at the European Union (EU), the provisions regarding the protection of personal data are found in the General Data Protection Regulation (GDPR). This regulation was

approved in 2016 and was implemented in 2018. The applicability of GDPR is not limited to countries in the European Union, but recommendations related to the provisions of GDPR are also implemented by several countries and international organizations around the world, including Indonesia. As a result, GDPR can be effective even outside the European Union, especially the United States. In addition to the GDPR, there is another major legal guideline in the EU governing data protection, namely the Council of Europe's Modernized Convention for the protection of data of individuals in connection with the Processing of Personal Data. According to these provisions, personal data is data that directly or indirectly identifies an individual and is considered sensitive data if the type of data is likely to have an impact on the fundamental rights and freedoms of individuals (Yuniarti, 2019). Therefore, health data falls into a special category of data, which is also referred to as sensitive data. Health data is defined as data that reveals information about a person's health. Then, in relation to the processing of personal data, the GDPR specifies that processing must be lawful, fair, and transparent, and consent must be obtained from the data subject. The GDPR defines processing as activities performed on personal data, such as collection, recording, organization, structuring, storage, alteration, retrieval, use, disclosure, carried out automatically or otherwise, by means of data transfer or dissemination or by other means such as data combination, restriction, and deletion (Nasution, 2020).

If processing is done without a legal basis, it is considered unlawful. This is what requires most health apps and wearables to have extensive privacy policies, which describe what data is collected, how it will be used, and with whom it is shared. In order to protect these activities, the GDPR provides that processing is unauthorized if it is not carried out in accordance with Article 9 and Article 32 of the GDPR, which essentially provide that all measures for data protection have been applied and the data subject has explicitly given consent (Fikri & Rusdiana, 2023).

Based on the description above, it is clear that in wearable technology devices, the data recorded and collected is not only limited to the user's health data but also other data such as personal activities and the user's environment. These activities certainly pose a great risk regarding the privacy of its users and therefore require a legal certainty that is able to provide protection for the personal data of data subjects. For this reason, this research will discuss the protection of personal data both before and after the enactment of the PDP Law, along with its comparison with the provisions applicable in the European Union through its provisions, namely the General Data Protection Regulation (GDPR). As such, this research aims to provide a comprehensive legal analysis of the implementation of personal data protection regulations on wearable technology, particularly in Indonesia and the European Union. This research seeks to identify the strengths and weaknesses of Indonesia's Personal Data Protection Law (PDP Law) compared to the European Union's General Data Protection Regulation (GDPR). In doing so, this research will highlight the key legal principles, enforcement mechanisms, and potential

improvements needed to strengthen personal data protection in Indonesia's regulatory framework.

The benefits of this research are twofold. First, this research will contribute to the academic discourse on digital privacy and personal data protection by offering a comparative legal perspective. By analyzing the similarities and differences between the PDP Law and GDPR, this research will provide insights into best practices and possible regulatory improvements for Indonesia. Secondly, this research will be a valuable resource for policymakers, legal practitioners, and technology users by providing recommendations on how wearable technology regulations can be enhanced to ensure better data security and user privacy protection. Findings from this research can guide future legislative developments, raise public awareness, and assist stakeholders in implementing more effective data protection measures in the rapidly evolving digital landscape.

RESEARCH METHOD

The research method used in this research is normative juridical, namely by conducting studies on the application of legal rules and norms based on secondary data, namely Law Number 23 of 2006 concerning Population Administration, as amended by Law Number 24 of 2013, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, and Law Number 27 of 2022 concerning Personal Data Protection. Furthermore, the typology of research in this writing is normative research, namely research analyzing existing legal events, using existing legal theories and norms to then be able to present perfect research and new circumstances in the research.

RESULT AND DISCUSSION

Personal Data Protection on Wearable Technology before the enactment of the Personal Data Protection Law

Personal Data Protection on Wearable Technology

Nowadays, data usage, data digitization, and effective data transfer are basic needs for every human being. For this reason, it is important to guarantee the protection of an individual's personal information with the sole purpose of ensuring that the absolute right to privacy of each individual is maintained. The idea of data protection, in principle, stems from the understanding that every individual has the right to freely transfer their personal information, and this right also includes the freedom to determine the conditions in the process of transferring personal data (Rosadi, 2023). Therefore, the protection of the personal data of each individual plays a very important role because it contains the principle of freedom and self-image of each individual,

whose implementation is a strong support for the achievement of freedom to be able to do whatever he wants.

One of the trends that are currently experiencing development is Wearable Technology, Wearables, Wearables Devices or known as Quantified Self Thing which is part of the Internet of Things (IoT) or smart things (smart devices), is a device equipped with many sensors embedded in it and connected to an object or individual (Thierer, 2014). This device is designed to be able to record, process, store, and transmit data by utilizing network connections, this device can interact with other devices and systems. The wearable device in this case can be an electronic device, small cellular, or computer accompanied by wireless communication capabilities to then be included in gadgets, accessories, or clothing used on the human body, or even in other versions such as micro-chips or smart tattoos. This technology is different from smartphones or tablets, because there is added value in these devices, namely various features that can perform monitoring and scanning, including biofeedback or other sensory physiological functions such as those related to biometry, which will continue to run, but limited by the battery capacity of the device.

Wearable Technology can be in the form of smartwatches, conventional sports trackers, on-body cameras, heart rate meters, and eye-wear, even in the future these devices will also involve various smart clothes and industrial equipment that are virtual in nature with enhanced versions (Seneviratne et al., 2017). While the main motivation presented by this technology is the drive to provide proactive problem solving in handling several things such as health care, fitness, aging prevention, people with disabilities, education, transportation, business (company), finance, entrance system, entertainment, music, and others, because this device is designed with the aim of handling problems, for example in the health sector it can be used to overcome the possibility of health problems of its users.

Besides the many functions and services offered, Wearable Technology also records and collects various personal activity data, including physiological data, activity data, and user environment data (de Arriba-Pérez et al., 2016). For those who aim to monitor their health, in addition to these data, these devices also record personal information such as heart rate, blood pressure, blood sugar, cholesterol, weight, personal activity range, schedule and habits and other user information.

As described earlier, Wearable Technology works by collecting highly personal and sensitive data, which can provide detailed information about a person's personal daily activities. This causes privacy issues to arise in the data collected and processed, in addition to the various benefits obtained from the application of its functions. While wearable technology collects data of a personalized nature with problem-solving as its processing output, the data is stored and processed by domestic and foreign service providers (companies), which may lead to issues regarding the data processing activities. In addition, there is a possibility for the wearable technology service provider to transfer the data to other third-party companies directly affiliated

with the service provider and get consistent service compensation from them and the possibility for hackers to directly obtain user data, resulting in the risk of leakage of users' personal data related to health issues, living habits and the range of user activities.

In the use of wearable devices, there are circumstances where the user gives permission to other parties (controllers) to process their data. In such conditions, there must be an agreement between the user and the manufacturer or application provider on the Wearable Technology device, which explicitly states the party who owns the data and how the data can be accessed or used by other parties, as well as the possibility of data uploaded to the cloud provided by the company. Therefore, it is expected that not only the controller can be responsible for processing and understanding the agreement, but the user is also responsible for understanding their data in using wearable technology devices, because by using this device, it indicates that users must be willing to give up some or even all control over their data as a form of real replacement for the benefits obtained from the device.

Personal Data Protection in relation to Wearable Technology before the enactment of the Personal Data Protection Law

Prior to the issuance and enactment of the Law on Personal Data Protection (UU PDP), in Indonesia there were no regulations that specifically regulated the protection of personal data. Provisions relating to this matter are scattered in several laws and regulations such as Law Number 23 of 2006 concerning Population Administration, as amended by Law Number 24 of 2013, which states that personal data is data belonging to each individual whose nature must be stored, maintained, kept correct and its confidentiality protected. The personal data in question is data related to Family Card Number, Population Identification Number (NIK), date or month or year of birth, information about physical conditions (physical or mental disabilities), NIK of biological mother and father, and some important history. This provision only regulates personal data within the scope of the definition and types of personal data in the context of population, while provisions regarding the collection, processing, and storage of data are not regulated (Djafar, 2019). Furthermore, Law No. 11/2008 on Electronic Information and Transactions (ITE Law) as amended by Law No. 19/2016, more clearly regulates that the use of a person's personal data through electronic media must always be based on the consent of the party concerned. Violation of this provision gives rise to a right of action for the party who feels their rights have been violated for all the losses they receive. In addition, it is also regulated that based on the request of the party concerned or with a court order, the electronic system organizer is obliged to delete electronic information and electronic documents under its control that are no longer relevant, along with the procedures for deleting electronic information and electronic documents.

Although the ITE Law does not explicitly regulate the definition of personal data, this provision indirectly regulates that the protection of personal data in the use of information

technology is one of the efforts to realize personal rights (privacy rights) which has a definition, namely:

a) The right to be free from all kinds of harassment and the right to enjoy life;
b) The right to be able to connect with other parties without any indication of surveillance; and
c) The right to monitor access to information relating to one's private life and data

In addition to the Adminduk Law and ITE Law, there are other laws and regulations, namely Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions (PP No. 71/2019) and Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20/2016 on the Protection of Personal Data in Electronic Systems (Permenkominfo No. 20/2016) which are sufficient to regulate the definition of personal data, personal data protection, and personal data processing. These two provisions regulate the same thing, that basically personal data is data relating to individuals who are identified or can be identified through analysis of other information either directly or indirectly with electronic or non-electronic systems. Furthermore, the protection of personal data on electronic systems includes protection in the process of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, disseminating, and destroying personal data. In carrying out these actions, Permenkominfo No. 20/2016 regulates that the electronic system used must have been verified, in addition, all actions must be carried out based on the consent of the owner of the personal data and first verify the accuracy of the data so that processing and analysis can be carried out in accordance with the purpose and purpose. As a form of appreciation of the data subject for the privacy of his/her personal data, the data subject is entitled to the confidentiality of his/her data, and to make changes to his/her personal data such as changes, additions and updates, file a complaint, obtain a history of the transfer of his/her personal data to the organizer, and data destruction. Personal data can be obtained and collected directly or indirectly through the adaptation of various data sources and must be verified immediately to the data owner. Then, in the event of a failure to protect the personal data of the data owner, the organizer is obliged to notify the owner of the personal data.

PP No. 71/2019 regulates that activities related to the management, processing and storage of data by public scope organizers (state agencies), must be carried out in the territory of Indonesia, except if storage technology is no longer available, then these activities can be carried out outside the territory of Indonesia, while in private scope organizers (individuals, business entities, or communities), these activities can in principle be carried out both inside and outside the territory of Indonesia, with the obligation of the organizer to ensure that supervision by the Ministry and law enforcement agencies has been carried out effectively (ZELAFIARA, 2022).

In relation to violations of unlawful processing activities, Permenkominfo No. 20/2016 and PP No. 71/2019 regulate the same thing, namely that the Minister or supervisory agency is

responsible for ensuring the implementation of these provisions, therefore if there are indications of violations, the parties concerned may be subject to administrative sanctions.

Personal Data Protection in relation to Wearable Technology under the General Data Protection Regulation (GDPR)

In the European Union (EU), there are two main legal provisions governing data protection, namely the General Data Protection Regulation (GDPR) and the Council of Europe's Modernized Convention, which regulates the protection of personal data in relation to personal data processing activities (Modernized Convention 108). Modernized Convention 108 has been in existence since 1982 and its provisions are more far-reaching when compared to the GDPR, as not only European countries are part of the convention, but also non-European countries.

As stipulated in Article 4 paragraph (1) of the GDPR, personal data is any information relating to an identified or identifiable individual (data subject). An identifiable data subject is an individual who can be identified either directly or indirectly on the basis of name, identification number, location, online identity, or one or more other more specific factors such as physical, physiological, genetic, mental, economic, cultural, or social characteristics of the individual. The GDPR stipulates that there are personal data of a highly sensitive nature, which require special protection in the context of their processing because they are closely related to the fundamental rights and freedoms of data subjects. Therefore, the determination of sensitive personal data plays an important role because personal data in this class has quite different provisions from other personal data. The difference lies in the freedom of the data subject to determine their own information and the level of control over their personal data, and the existence of special provisions relating to the requirements in the processing of their data.

Sensitive personal data includes data indicating racial or ethnic origin, political views, beliefs, occupational membership, genetic data and biometric data aimed at identifying a person, health data, and sexual or orientation data (ZELAFIARA, 2022). Furthermore, the GDPR stipulates that health data is personal data relating to a person's physical and mental health, and also includes health care providers, who disclose information about health status. As such, health data is considered sensitive personal data which contains a lot of information about a person's health. Meanwhile, in relation to the source of information about health data, it is not limited to medical instruments, so that if the information is sourced on devices such as wearable technology, it can also be included in sensitive personal data.

The GDPR provides that processing is any act of collecting, recording, organizing, storing, transforming and disclosing personal data by any means automated or otherwise. Processing must be lawful, transparent and fair, data collection and processing limited to specific purposes, accurate, data retention for a limited time and data confidentiality preserved.

As stipulated in Article 9 Paragraph (1) of the GDPR, the processing of personal data belonging to the sensitive category is basically prohibited, but there are exceptions if the processing meets the conditions as stipulated in Article 9 Paragraph (2) of the GDPR, such as

having obtained the prior consent of the data subject and for special purposes such as in the health sector, namely to carry out medical diagnosis, treatment, public interest, and scientific research. This consent must be given by an actual act that indicates freely and clearly that the data subject has consented to the processing of his or her personal data. Also, appropriate data protection has been carried out as stipulated in Article 32 of the GDPR, which includes masking measures and encryption of personal data. The GDPR does not regulate the systematics of giving consent, so there is no prohibition for data providers to give it by electronic means, only that the request for consent must be unequivocal, simple and unobtrusive, whereas the evidence of receipt by the data subject must clearly indicate that the proposed processing has been consented to by the data subject. Article 7 of the GDPR further provides that, in relation to processing, the party must be able to prove the data subject's consent to the processing of his or her personal data, as well as the data subject's right to withdraw his or her consent at any time, in a manner that is as straightforward as the process for giving consent.

The GDPR further provides that processing shall be carried out in a transparent manner with due regard to the rights of data subjects through the provision of information including:

a) Identity of the controller and data protection, purpose of processing, recipients of personal data, as well as information if the controller wishes to transfer data to a third party;
b) The rights of data subjects which include the right of access, to exercise and obtain notice in the event of data rectification, to delete data, to restrict processing, data transfer, to object, and not to be subject to decisions based on automated processing, and other restrictions based on Union or Member State law;
c) Inform if there is a personal data breach on the data subject.

The GDPR defines a personal data breach as a breach of security that results in the accidental and unlawful destruction, loss, alteration, unauthorized disclosure of personal data, or unauthorized access to personal data. As for the problem of personal data breaches in relation to wearable technology, it can usually involve several countries, especially now that wearable technology is widely used in data subjects around the world, as for the health data collected by wearable technology, it can pose various risks such as use or sale for commercial purposes, data can be transferred and stored anywhere such as company partners, service providers and other partners regardless of national boundaries that record user data to be sent to the cloud or company servers, which makes it difficult to track data movement afterwards. Thus, the GDPR provides protection by stipulating that the GDPR applies to the processing of personal data subjects who are within the EU but whose controller or processing party is outside the EU, where the processing activity relates to the offering of products or the monitoring of the data subject's behavior.

As for the GDPR, it applies worldwide to data subjects located in the EU. However, in its implementation, there are certainly problems regarding jurisdiction that are incompatible with the legal system in non-EU countries, for this reason, the GDPR stipulates that the transfer of

personal data involving the transfer of data to third countries or international organizations can only be carried out if all provisions in the GDPR, especially Chapter 5 on the transfer of personal data to third countries or international organizations, have been fulfilled, in order to ensure the protection of data subjects, namely by (1) ensuring that the recipient of the data has an adequate level of security (Article 45 GDPR), through the fulfillment of adequate conditions or the provision of derivative provisions that ensure that the country or international organization is obliged to provide adequate data protection assurance accompanied by the possibility of periodic review thereof. (2) the controller or processor ensures appropriate safeguards (Article 46 GDPR), and (3) binding corporate provisions (Article 47 GDPR).

Further, in principle, if a data subject alleges a breach in data processing, the GDPR provides that the data subject has the right to lodge a complaint with a supervisory authority, namely in the country of the data subject or where the alleged breach occurred, in addition to administrative and other legal remedies.

Thus, before the issuance of regulations that specifically regulate the protection of personal data in Indonesia at the level of the Law, Indonesia through the laws and regulations under it has sufficiently provided legal certainty with regard to the protection of personal data as stipulated in the GDPR which became a reference provision for Indonesia before the issuance of the PDP Law, but the provisions are still very limited and lack specific provisions with regard toFirst, the explanation related to the type of personal data. Whereas through the legislation at that time, personal data was only defined as data about an identified or identifiable individual, when referring to the GDPR, the most important discussion in personal data is to determine the type of personal data itself, because for personal data that falls into the category of sensitive data, there are different provisions in processing, which basically all processing activities are not allowed, but with the fulfillment of several requirements, then processing for sensitive personal can be done, Second, Second, provisions relating to processing activities carried out involving third parties located outside the territory of Indonesia have indeed been regulated, but the existing statutory provisions do not regulate the existence of differences in jurisdiction that may conflict with Indonesia, unlike the GDPR, this is regulated in a special chapter that regulates the transfer of personal data to third countries or international organizations, which requires data transfers to be carried out by ensuring that the recipient of the data has an adequate level of security, the controller or processor ensures proper security, and there are binding corporate provisions.

Protection of Personal Data on Wearable Technology after the enactment of the Personal Data Protection Law

As a concrete form of the mandate of the 1945 Constitution in Article 28G paragraph (1) which stipulates that, every individual is entitled to obtain personal protection, family, honor, dignity, and wealth that belongs to him, and is entitled to enjoy a sense of security from threats to do or not do something that is his human right. Therefore, Law Number 27 Year 2022 on

Personal Data Protection (UU PDP) was issued as a form of protection of one of the human rights, namely the security of personal data of each individual.

The PDP Law defines personal data as a set of data relating to an individual, which is identified or can be identified by itself or by the presence of supporting factors, namely by electronic or non-electronic systems directly or indirectly (Penyusun et al., 2021). Meanwhile, what is meant by personal data protection is all activities in order to provide personal data protection for personal data processing activities in order to provide guarantees for the constitutional rights of personal data subjects. Personal data is divided into two types, namely specific and general personal data. Data related to health, biometrics, and genetics are specific personal data. Specific personal data in its processing may pose a greater risk to the subject of personal data, namely the possibility of discrimination or harm.

Personal data processing activities include obtaining and collecting, processing and analyzing, storing, correcting and updating, displaying, publishing, transferring, disseminating or disclosing as well as deleting or destroying personal data, the implementation of which is limited and specific, legally guaranteed, and transparent, in line with the purpose of the processing, the rights of the data subject are guaranteed, accurate and accountable with clear evidence, preceded by notification (purpose and processing activities, as well as notification of data protection failure).

In the processing of personal data, it must always be based on the express consent of the data subject for a specific purpose that has been informed in advance by the personal data controller, as well as some fulfillment of legitimate interests stipulated in the PDP Law. With regard to consent in the context of data processing, the controller is obliged to provide information regarding the basis, purpose, type of data and its relation to the processing activity, deadlines for document retention, detailed description of the information collected, duration of processing, rights of the data subject, which can be done either in written or recorded form and can be submitted electronically or non-electronically.

The rights of data subjects in the PDP Law are regulated from Article 5 to Article 13, including the right to obtain information on the party requesting the data, to make data replacement, access to a copy of the data, terminate processing and delete the data, withdraw consent, file an objection, restrict processing, sue, use and send their personal data to the controller, where the right to make corrections, updates, and improvements, the right to obtain access to a copy, the right to terminate and delete processing, the right to withdraw consent, and the right to file an objection, need to be requested in a recorded manner to the data controller either electronically or non-electronically.

In the PDP Law, provisions regarding the transfer of personal data are regulated in a separate chapter. Where the personal data controller can transfer personal data to personal data controllers both located in Indonesia, as well as to personal data controllers and processors outside the jurisdiction of Indonesia, based on the applicable legislation. As for the transfer of

data outside the jurisdiction of Indonesia, Article 56 of the PDP Law stipulates that the controller is obliged to ensure that the recipient country has an equivalent or even higher level of personal data protection, or if not, there is an obligation of the personal data controller to ensure that there is adequate and binding protection of personal data. Alternatively, if these requirements cannot be met, the data transter must at least obtain the consent of the data subject.

It is further stipulated that the responsibility for the processing of personal data shall be borne by the controller of personal data. Meanwhile, if there is a failure in the protection of personal data, the controller is obliged to make a written notification to the data subject and the institution, which contains a notification of the disclosed personal data along with a description of the time and explanation of the event, as well as efforts in order to handle and restore the data, no later than 3x24 hours.

The PDP Law provides administrative sanctions for violations of the provisions as stipulated in the PDP Law (Penyusun et al., 2021). The administrative sanctions can be in the form of written warnings, temporary suspension of personal data processing activities, or administrative fines.

Thus, after the enactment of the PDP Law, the regulations relating to the protection of personal data are clearer and clearer. In relation to wearable technology, the provisions in the PDP Law are broadly similar to those in the GDPR, even in certain provisions, namely in the case of processing consent, the PDP Law more explicitly regulates that consent can be made either in written or recorded form which can be submitted electronically or non-electronically.

What is quite different from the provisions in the GDPR is in data transfers involving countries or international organizations, where the GDPR stipulates that the controller is obliged to ensure that the data recipient has an adequate level of security the controller or processor ensures the existence of appropriate safeguards, and the existence of binding corporate provisions. The adequate level of security can be provided by the fulfillment of adequate conditions, or the provision of derivative provisions that ensure that the country or international organization is obliged to provide adequate data protection assurance, accompanied by the possibility of periodic review. Unlike the PDP Law, which does not provide further provisions regarding the qualification of the level of protection of personal data that is equal to or even higher than the country or international organization receiving the data.

CONCLUSION

The conclusion of this study highlights the significant differences between Indonesia's Personal Data Protection Law (PDP) and the General Data Protection Regulation (GDPR). The absence of a clear classification of personal data in the PDP Law poses a challenge, as the GDPR places significant emphasis on distinguishing between general and sensitive personal data, each of which has different regulatory requirements. In addition, the PDP Law does not have specific provisions regarding the transfer of personal data to third parties outside of Indonesia, unlike the GDPR, which sets out strict requirements to ensure that the recipient of the data maintains an

adequate level of protection. The regulation of cross-border data transfers in the PDP Law is still inadequate, especially regarding mechanisms to ensure that the receiving country or organization upholds the same or higher level of data protection. These differences indicate potential legal gaps that may impact the implementation of data protection in Indonesia, especially in cases of international data exchange.

Future research should explore how Indonesia can adopt a more comprehensive data protection framework that aligns with international best practices while addressing the country's unique legal and technological landscape. Further research could focus on formulating policy recommendations for cross-border data transfers to ensure legal certainty and adequate security measures. Additionally, an in-depth comparative analysis between the PDP Law and data protection laws from other jurisdictions may provide insights to improve regulatory mechanisms to enhance privacy protection in Indonesia. These findings contribute to the ongoing discussion on strengthening data governance and ensuring compliance with global data protection standards.

REFERENCES

Aroganam, G., Manivannan, N., & Harrison, D. (2019). Review on wearable technology sensors used in consumer sport applications. *Sensors*, *19*(9), 1983.

Aswathy, S. U., & Tyagi, A. K. (2022). 10 Privacy Breaches. *Security and Privacy-Preserving Techniques in Wireless Robotics*, *163*.

Çiçek, M. (2015). Wearable technologies and its future applications. *International Journal of Electrical, Electronics and Data Communication*, *3*(4), 45–50.

de Arriba-Pérez, F., Caeiro-Rodríguez, M., & Santos-Gago, J. M. (2016). Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios. *Sensors*, *16*(9), 1538.

Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. *Seminar Hukum Dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM*, *26*.

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39–57.

Lee, J., Kim, D., Ryoo, H.-Y., & Shin, B.-S. (2016). Sustainable wearables: Wearable technology for enhancing the quality of human life. *Sustainability*, *8*(5), 466.

Nasution, T. H. (2020). *Perlindungan Hukum Data Pribadi Nasabah dalam Penggunaan Big Data Oleh Perbankan di Indonesia (Studi Komparatif Penggunaan Data Pribadi Nasabah di Uni Eropa)*.

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D. Q., Chukhno, N., & Chukhno, O. (2021). A survey on wearable technology: History, state-of-the-art and current challenges. *Computer Networks*, *193*, 108074.

Penyusun, T., IGJ, O. G., Saputra, A. F., & Aziz, M. F. (2021). *Perlindungandatapribadi Diindonesia*.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.

Sahib, N. S. M., Idayanti, S., & Rahayu, K. (2023). Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia. *Pancasakti Law Journal (PLJ)*, *1*(1), 61–74.

Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., & Seneviratne, A. (2017). A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials*, *19*(4), 2573–2620.

Sivakumar, C. L. V, Mone, V., & Abdumukhtor, R. (2024). Addressing privacy concerns with wearable health monitoring technology. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *14*(3), e1535.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142.

Thierer, A. (2014). The internet of things and wearable technology. *Mercatus Center or George Mason University*.

Vijayan, V., Connolly, J. P., Condell, J., McKelvey, N., & Gardiner, P. (2021). Review of wearable devices and data collection considerations for connected health. *Sensors*, *21*(16), 5589.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147–154.

Zelafiara, E. G. A. (2022). *Kebijakan Formulasi Terhadap Kebocoran Data Pribadi Berdasarkan Rancangan Undang-Undang Perlindungan Data Pribadi*.

Copyright holder:
Erika Leony, Tjhong Sendrawan (2025)

First publication right:
Asian Journal of Engineering, Social and Health (AJESH)

This article is licensed under: