Journal of Law and Regulation Governance

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]
Fakultas Hukum, Universitas Indonesia, Indonesia
Email: erikaleonyy26@gmail.com

ABSTRACT

Wearable Technology is a device that works by recording and collecting various user data such as personal activity and physiological and environmental data. This data enables users to monitor and manage their health with the abundance of personal information provided. Despite its benefits, wearable technology poses potential risks to privacy and data security. Given the sensitivity and confidentiality of health-related personal data, it is crucial to emphasize privacy in wearable technology. The enactment of the Personal Data Protection Law (UU PDP) aims to provide legal certainty for Indonesian citizens against potential digital crimes. Through a comparative study with the provisions applicable in the European Union (EU), this paper analyzes the conception of personal data protection in wearable technology. The findings reveal that the EU's General Data Protection Regulation (GDPR) provides a more comprehensive framework, highlighting areas where Indonesia's UU PDP could be enhanced. Recommendations include adopting stricter data management protocols and raising public awareness to mitigate privacy risks associated with wearable technology.

Keywords: Personal Data Protection, Wearable Technology

INTRODUCTION

Technology continues to evolve, driven by the demand for innovative services and the rapid pace of digital advancements (Müller & Shamsie, 2023). One notable development is "wearable technology," which has become an integral part of modern life. Devices like smartwatches, fitness trackers, and wearable health monitors offer real-time insights into users' health and activities, simplifying daily routines and increasing productivity. These devices integrate advanced features such as health monitoring and data tracking, making them indispensable tools for many individuals (YIN et al., 2016).

While wearable technology offers significant benefits, such as improved health management and accessibility to information, its data collection capabilities raise critical concerns about personal data protection (Sivakumar et al., 2024). These devices continuously record and process sensitive user information, including health metrics, personal activities, and environmental data. This extensive data collection, while useful, introduces significant risks to user privacy and security.

For instance, investigations have revealed that some applications associated with wearable devices share user data with third parties without adequate transparency or consent. Such practices

expose users to unauthorized access, potential data breaches, and misuse of sensitive information. Privacy concerns are heightened by the ability of wearable devices to operate discreetly, capturing personal data continuously and sometimes without the user's awareness (O'Hagan et al., 2023).

In Indonesia, legal frameworks for personal data protection, such as the recently enacted Law No. 27 of 2022 on Personal Data Protection (UU PDP), provide clearer guidelines on safeguarding sensitive information. This law classifies personal data into specific and general categories, with health data and other biometric information falling under the specific category due to their sensitive nature (Chua et al., 2021). Data processing activities must adhere to strict principles, including obtaining explicit user consent, ensuring data security, and preventing unauthorized use.

Globally, regulations like the European Union's General Data Protection Regulation (GDPR) set rigorous standards for data processing, emphasizing transparency, legality, and user consent (Tikkinen-Piri et al., 2018a). The GDPR's influence extends beyond the EU, serving as a benchmark for international data protection practices. These provisions highlight the critical need for stringent privacy policies and legal safeguards to address the vulnerabilities inherent in wearable technology.

This research aims to explore the legal frameworks governing personal data protection in wearable technology, comparing Indonesia's UU PDP with the EU's GDPR. By examining these regulations, the study seeks to provide insights into ensuring robust data protection mechanisms while accommodating technological advancements (Shandilya et al., 2024).

RESEARCH METHODS

The research method employed in this study is normative juridical, which involves analyzing the application of legal rules and norms based on secondary data. This includes examining 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. The choice of the normative juridical method is particularly relevant to the research objectives as it allows for a structured analysis of legal events, using established legal theories and norms to provide a comprehensive understanding and generate new insights aligned with the research goals. Additionally, the typology of this research emphasizes normative analysis, enabling a robust examination of existing legal frameworks to address the identified issues effectivel (Sovacool et al., 2018).

RESULTS AND DISCUSSION

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

a. 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. 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. 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 (Nahavandi et al., 2022). 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 (Indrakumari et al., 2020). 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 (Poongodi et al., 2020). 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 (Banerjee et al., 2018). 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 (Muzny et al., 2020). 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.

b. 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 (Sudarwanto & Kharisma, 2022). 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. 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 (Silva & MA, 2017). 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 (Rustad & Koenig, 2019).

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.

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.

c. 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 (de Terwangne, 2022).

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 (Tikkinen-Piri et al., 2018b). 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. 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 (Thapa & Camtepe, 2021). 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 (Dankar et al., 2019). 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 (Pimenta Rodrigues et al., 2024). 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 (Syailendra et al., 2024). 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 (Bartolini & Siry, 2016) .

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. 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 Personal Data Protection (PDP) Law in Indonesia demonstrates several significant differences compared to the GDPR, particularly in its level of detail and scope. First, the PDP Law does not provide a clear explanation regarding the categorization of personal data, despite the GDPR emphasizing this aspect as crucial. Sensitive personal data, under the GDPR, is subject to specific processing provisions, highlighting the importance of such categorizations in ensuring robust data protection measures. Second, while the GDPR dedicates a specific chapter to the transfer of personal data to third countries or international organizations, including provisions to ensure that the recipient has adequate security measures in place, the PDP Law lacks comparable clarity. It does not address potential jurisdictional conflicts when third parties outside Indonesia are involved.

One of the most critical omissions in the PDP Law lies in its lack of detailed provisions concerning the qualification of data protection standards. Unlike the GDPR, which requires that data transfers occur only if the recipient country or organization meets an equivalent or higher level of data protection, the PDP Law does not provide guidelines or benchmarks for assessing such adequacy. To align with international best practices and enhance its regulatory framework, future amendments to the PDP Law should incorporate specific provisions addressing these gaps. This includes defining the types of personal data, establishing jurisdictional guidelines for cross-border processing, and adopting a mechanism to evaluate and ensure the adequacy of protection in recipient countries or organizations.

REFERENCES

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society*, *34*(1), 49–57.

Bartolini, C., & Siry, L. (2016). The right to be forgotten in the light of the consent of the data subject. *Computer Law & Security Review*, *32*(2), 218–237. https://doi.org/10.1016/j.clsr.2016.01.005

Chua, H. N., Ooi, J. S., & Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*, *110*, 102453. https://doi.org/10.1016/j.cose.2021.102453

Dankar, F. K., Gergely, M., & Dankar, S. K. (2019). Informed Consent in Biomedical Research. *Computational and Structural Biotechnology Journal*, *17*, 463–474. https://doi.org/10.1016/j.csbj.2019.03.010

de Terwangne, C. (2022). Privacy and data protection in Europe: Council of Europes Convention 108 and the European Unions GDPR. In *Research Handbook on Privacy and Data Protection Law* (pp. 10–35). Edward Elgar Publishing.

Indrakumari, R., Poongodi, T., Suresh, P., & Balamurugan, B. (2020). The growing role of Internet of Things in healthcare wearables. In *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach* (pp. 163–194). Elsevier. https://doi.org/10.1016/B978-0-12-819593-2.00006-6

Müller, S., & Shamsie, K. (2023). Digital Disruption and the Evolution of Business Models: A Scholarly Examination. *Abbottabad University Journal of Business and Management Sciences*, *1*(01), 43–52.

Muzny, M., Henriksen, A., Giordanengo, A., Muzik, J., Grøttland, A., Blixgård, H., Hartvigsen, G., & Årsand, E. (2020). Wearable sensors with possibilities for data exchange: Analyzing status and needs of different actors in mobile health monitoring systems. *International Journal of Medical Informatics*, *133*, 104017. https://doi.org/10.1016/j.ijmedinf.2019.104017

Nahavandi, D., Alizadehsani, R., Khosravi, A., & Acharya, U. R. (2022). Application of artificial intelligence in wearable devices: Opportunities and challenges. *Computer Methods and Programs in Biomedicine*, *213*, 106541. https://doi.org/10.1016/j.cmpb.2021.106541

O'Hagan, J., Saeghe, P., Gugenheimer, J., Medeiros, D., Marky, K., Khamis, M., & McGill, M. (2023). Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *6*(4), 1–35.

Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. de, de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. *Data*, *9*(2), 27.

Poongodi, T., Krishnamurthi, R., Indrakumari, R., Suresh, P., & Balusamy, B. (2020). Wearable devices and IoT. *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, 245–273.

Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Fla. L. Rev.*, *71*, 365.

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the Regulatory Landscape. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (pp. 127–240). Springer.

Silva, S., & MA, L. L. M. (2017). *Personal and Non-Personal Data in the Context of Big Data*.

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.

Sovacool, B. K., Axsen, J., & Sorrell, S. (2018). Promoting novelty, rigor, and style in energy social science: Towards codes of practice for appropriate methods and research design. *Energy Research & Social Science*, *45*, 12–42. https://doi.org/10.1016/j.erss.2018.07.007

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457.

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indon. L. Rev.*, *14*, 175.

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018a). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018b). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

YIN, Y., Zeng, Y., Chen, X., & Fan, Y. (2016). The internet of things in healthcare: An overview. *Journal of Industrial Information Integration*, *1*, 3–13. https://doi.org/10.1016/j.jii.2016.03.004