Universitas Internasional Batam
Fakultas Hukum
Jl. Gadjah Mada, Batam, 29442, Indonesia
Phone : (0778) 743 7111 Ext, 140.
Email: admin_jlpt@gmail.com

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

PERSONAL DATA PROTECTION IN TELEMEDICINE: COMPARISON OF INDONESIAN AND EUROPEAN UNION LAW

Miftahul Jannah[*], F. Yudhi Priyo Amboro[**], Rina Shahrullah[***]
Universitas Internasional Batam

Abstract

Telemedicine allows patients to receive remote medical consultation, diagnosis, and treatment through a digital platform. However, with the development of telemedicine, personal data protection has become one of the main concerns. This research aims to compare the regulation of personal data protection in telemedicine services in Indonesia and the European Union. The type of research in this scientific article is Normative Juridical Research with a comparative legal approach. The data sources obtained in this paper are primary data and secondary data. The data collection method is a literature study. The data analysis method in this paper uses a qualitative approach. The results show that personal data protection in Indonesia is regulated by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). While in the European Union, Personal Data Protection is regulated in the General Data Protection Regulation (GDPR) which regulates the collection and use of personal data by organizations. Some similarities in personal data protection in both telemedicine in Indonesia and in the European Union are that the same consent requires telemedicine providers to obtain clear and explicit consent from patients. Both telemedicine providers must not disclose the patient's personal data to third parties without the patient's consent. Telemedicine providers to implement security measures to protect patient personal data. Both Indonesia and the European Union give patients the right to access, correct, delete, and limit the use of their personal data

Keywords: *diversion; ABH; law; Indonesia; the Beijing rules*

A. Background

Globalization requires the world to continue to move towards modernization, thus encouraging the emergence of various innovations in the field of technology and information [1]. Information technology has changed people's lifestyles globally and caused significant socio-cultural, economic, and legal framework changes. Although internet penetration in the community is still very less when compared to the total population of Indonesia, now, electronic information and communication systems have

[*] mjannah3008@gmail.com

[1] Inaz Indra Nugroho, Reza Pratiwi, and Salsabila Rahma Az Zahro, 'Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia', *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 1.2 (2021), 115–29 <https://doi.org/10.15294/ipmhi.v1i2.53698>.

been implemented in almost all sectors of life in society, including the health sector [2].

In general, e-health consists of health informatics (*health informatics*) and telehealth efforts (*tele-health*). One of the implementations *tele-health* be *telemedicine. Telemedicine* is the provision of telehealth services by health professionals using information and communication technology, including the exchange of information on diagnosis, treatment, prevention of disease and injury, research and evaluation, and continuing education of health care providers for the benefit of improving individual and community health [3]. *Telemedicine* is the practice of health using audio, visual and data communication, including treatment, diagnosis, consultation and treatment as well as the exchange of medical data and remote scientific discussions. *Telemedicine* became evidence of increased access to information and medical care for patients, earning it the nickname "Remote Medical Services" [4].

Telemedicine is a method of health care providers where health practitioners / operators and patients are not in the same place, through the use of Technology, Information and Communication (ICT) [5]. *Telemedicine*, has experienced rapid development in recent years. Digital technology allows patients to consult with medical personnel, get diagnoses, and even undergo remote treatment through the platform *Online*. This provides significant benefits, especially for individuals who live in remote areas, have limited mobility, or need faster and more efficient access to health[6]. This provides significant benefits, especially for individuals who live in remote areas, have limited mobility, or need faster and more efficient access to healthcare.

The implementation of *telemedicine* in Indonesia is an effort to improve the quality of health service facilities with remote consultation services, especially remote areas. In *telemedicine*, human resources, facilities, infrastructure, equipment and applications are needed. The *telemedicine* application used must have a data security and safety system both provided by the Ministry of Health and independently developed that has been registered with the Ministry of Health. Telemedicine applications in

[2] Glenn Wijaya, 'Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum', *Law Review*, XIX.3 (2020), 326–61.
[3] Agus Riyanto, 'Faktor-Faktor Yang Mempengaruhi Pelaksanaan Telemedicine (Systematic Review)', *Jurnal Manajemen Informasi Kesehatan Indonesia*, 9.2 (2021), 174 <https://doi.org/10.33560/jmiki.v9i2.337>.
[4] D. Ferorelli, 'Medical Legal Aspects of Telemedicine in Italy: Application Fields, Professional Liability and Focus on Care Services During the COVID-19 Health Emergenc', *Italia : Journal of Primary Care and Community Health*, 11 (2020).
[5] D. Ferorelli and others, 'Medical Legal Aspects of Telemedicine in Italy: Application Fields, Professional Liability and Focus on Care Services During the COVID-19 Health Emergency', *Journal of Primary Care and Community Health*, 11 (2020) <https://doi.org/10.1177/2150132720985055>.
[6] Hsiao Han Lu and others, 'A Study Investigating User Adoptive Behavior and the Continuance Intention to Use Mobile Health Applications during the COVID-19 Pandemic Era: Evidence from the Telemedicine Applications Utilized in Indonesia', *Asia Pacific Management Review*, 28.1 (2023), 52–59 <https://doi.org/10.1016/j.apmrv.2022.02.002>.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

Indonesia are quite rapidly developing, Indonesian people have various application options that can be used to get remote health consultation services (Surya &; Kur'aini, 2022). While in Europe, WHO reported the latest data that provides an overview of the development and benefits of using *telemedicine*, with 29 cases from all regions in Europe (Pharmacotics, 2016). One of the obligations of health care facilities as a provider of consultations in *telemedicine services* is to maintain the confidentiality of patients' personal data.

However, with the advancement of technology *telemedicine*, concerns have also been raised regarding the protection of patients' personal data. At this time, the information is already considered as *"power"* which is interpreted as power and power that greatly determines the fate of humans themselves. Currently, people's dependence on information technology is getting higher so that the higher the risks faced. Information technology is currently a "double-edged sword" because in addition to contributing to the improvement of welfare, progress and human civilization, it is also an effective means of unlawful acts including criminal acts (crimes). These various forms of criminal acts (crimes) have come to be known as "*cybercrime*". When discussing cybercrime with regard to personal data leakage, it basically refers to individual privacy. Especially in this era of big data, various applications and data collection devices are widespread and diverse communication technologies (such as, *Powerline Communications*, mobile networks, Internet and sensor networks) have provided and tremendous efficiency to collect a host of individual data which includes individual identity, finances, physical condition, and livelihood [7].

The perception of personal data protection is related to the concept of privacy, where the concept of privacy itself is the idea of maintaining personal integrity and dignity, because the right to privacy includes the right to determine, provide or not provide personal data [8]. During the teleconsultation process, data transfer and storage of the patient's medical information becomes an important part of the process. Sensitive personal data, such as medical history, identity information, or laboratory test results, needs to be carefully managed and properly protected from falling into the wrong hands or being used unlawfully.

Previous research stated that Legal protection of personal data is very important. Indonesia's personal data protection rules are spread across various laws and regulations, but the increasing cases of misuse of personal data in

[7] Muhammad Rais Alfaridzi, 'Analisis Framing Pemberitaan Kasus Kebocoran Data Pribadi Di Media Online (Studi Deskriptif Analisis Framing Model Robert N Entman Pemberitaan Terkait Kasus Kebocoran Data Pribadi Oleh Hacker Bjorka Di Tempo.Co Dan Kompas.Com Periode 22 Agustus – 18 Novem', *Universitas Sebelas Maret*, 2022.
[8] Syafira Agata Ramadhani, Fakultas Hukum, and Universitas Brawijaya, 'Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa', *Jurnal Hukum Lex Generalis*, 3.1 (2021), 73–84.

Indonesia force the Personal Data Protection Bill to be passed immediately[9]. Personal data protection law is governed by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection in Electronic Systems and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). *Telemedicine* has also been regulated in the Minister of Health Regulation no. 20 of 2019 concerning the Implementation of Telemedicine Services Between Health Service Facilities which explains data security and safety. On the other hand, the European Union has endorsed *General Data Protection Regulation* (GDPR) which came into effect in May 2018, which became a comprehensive personal data protection standard in the region.

The General Data Protection Regulation (GDPR) is a general data protection regulation in law that constitutes the personal data protection of the European Union and the European Economic Area *(European Economic Area).* The GDPR has important components in personal data law, human rights and the discussion of transfers of personal data outside the European Union and European Economic Area. The main purpose of GDPR is to increase control and rights of individuals over personal data and simplify regulations in the scope of international business.[10]

In context *telemedicine*, the differences in personal data protection law between Indonesia and the European Union are important to study. Because *telemedicine* may involve cross-border data transfers, both between Indonesia and the European Union and between EU member states themselves, a clear understanding of the differences and suitability of applicable personal data protection laws is required [11].

This study aims to analyze the differences in personal data protection law between Indonesia and GDPR in the European Union in the context of *telemedicine*. By highlighting the differences and similarities between these two regulations, the study will provide a better understanding of personal data protection in *telemedicine* practice, as well as its implementation for healthcare providers and patients in both regions.

B. Research Methods

The type of research in this scientific article is Normative Juridical Research with a comparative legal approach. The comparative research method allows comparison of legal systems, policies, and practices applicable in two different areas (Ali, 2021). This comparative research method will

[9] Wan Indy Azka Arbella, 'Perbandingan Hukum Terhadap Perlindungan Data Pribadi Menurut Hukum Positif Indonesia Dan General Data Protection Regulation (GDPR) Uni Eropa', *Faculty of Law*, 2020.
[10] Council of the European Union, 'Interinstitutional File: 2012/0011 (COD)', 2015.June (2015), 201.
[11] Pujiyono Suwadi, 'Legal Comparison of the Use of Telemedicine between Indonesia and the United States', *International Journal of Human Rights in Healthcare*, 2022.

provide a deep understanding of the differences in personal data protection law between Indonesia and GDPR in the European Union on *telemedicine*. This approach enables comprehensive analysis and benchmarking of best practices, which in turn can contribute to the development of better personal data protection policies and practices in *telemedicine* in both regions. The sources of data obtained in this paper are primary data and secondary data. The data obtained is used to assist in providing answers to problems. Primary data and secondary data, in the form of:

1. Secondary Data

   Secondary data is obtained through documentation methods, namely data sources in the form of sources from images or videos, works, and written things that can provide information [12].

   a. Primary Legal Materials: The primary legal materials used in this study are Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Personal Data Protection in Electronic Systems and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Minister of Health Regulation Number 20 of 2019 concerning the Implementation of Telemedicine Services Between Health Service Facilities. While the GDPR used in this study is the Data Protection Act 1998, and the EU Data Protection Directive 1995.
   b. Secondary Legal Materials: Secondary legal materials used in this study such as journals, books, and research results related to personal data protection in Indonesia and the European Union.
   c. Tertiary Legal Materials: The tertiary legal materials used in this study include legal dictionaries, which will be used to clarify and explain legal terms relevant to personal data protection

   The data collection method is a literature study which is a collection of activities related to the method of collecting library data, reading, recording, and processing research materials [13]. In this data collection technique, researchers collect and analyze descriptive materials. The data analysis method in this paper uses a qualitative approach with a comparative legal approach in the field of law (Ramadany, 2023). The analysis will be conducted by comparing personal data protection in Indonesia and the European Union, as well as analyzing legal perspectives related to data protection in both countries. The research questions asked will be a guide in the data analysis process. The results of the analysis will be interpreted and compiled into a clear and structured description. The research findings will be described in the form of a narrative that describes a comparison

[12] Nilamsari.
[13] Zed.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

of personal data protection in Indonesia and the European Union, as well as related legal perspectives.

C. Results And Discussion

Similarities and Differences between Personal Data Protection in Indonesia and GDPR in the European Union on Telemedicine

Protection of personal data is important to maintain the privacy and security of individuals. In Indonesia, personal data protection is regulated by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This PDP Law is a law that regulates the protection of personal data of an individual nature, both identified and identifiable separately or combined with other information, either directly or indirectly through electronic and/or non-electronic systems [14]. While in the European Union, Personal Data Protection is regulated on *General Data Protection Regulation* (GDPR) which governs the collection and use of personal data by organizations. GDPR aims to give individuals more control over their personal data and to make organizations more accountable for how they handle personal data.

Personal data protection arrangements on both telemedicine in Indonesia and in the European Union have similarities. The following are some of these similarities:

Approval

1. GDPR
   a. Article 6(1)(a) GDPR states that the processing of personal data is permissible if the data subject gives consent to the processing for a specific purpose. Consent must be given voluntarily, specifically and informatively.
   b. Article 7 of the GDPR further explains the clear and explicit requirements for consent. Consent must be given voluntarily if the data subject has the freedom to choose whether or not to give consent. Consent must be specific if the data subject clearly understands what they are consenting to. Consent should be informative if the data subject has sufficient information about the processing of their personal data
2. PDP Act
   a. Article 6 paragraph (1) letter a of the PDP Law states that the processing of personal data can be carried out with the consent given by the owner of the personal data. Consent must be given voluntarily, specifically and informatively.
   b. Article 10 paragraph (1) of the PDP Law further explains the clear and explicit approval requirements. Consent must be given voluntarily if the owner of the personal data has the freedom to choose whether or not to give consent. Consent must be specific if the owner of the personal data clearly understands what they are consenting to. Consent should be informative if the owner of

[14] Muhamad Iqbal, 'Privacy Policy | Global Climate Change', *STIA LAN*, 2022, p. 1.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

the personal data has sufficient information about the processing of their personal data.

Both Indonesia and the European Union require telemedicine providers to obtain clear and explicit consent from Patients before collecting, using, and processing their personal data. Consent must be given voluntarily, specifically and informatively.

Confidentiality

1. GDPR
    a. Article 5(1)(e): Personal data must be processed securely in a manner that protects against accidental or illegal loss, misuse, unauthorized access, disclosure, alteration or destruction.
    b. Article 9(2)(a): The processing of sensitive personal data is permissible if the data subject gives specific, clear and informed consent.
2. PDP Act
    a. Article 26 paragraph (1): Controllers and processors shall implement effective protection of personal data through the implementation of a series of engineering and organizational measures to ensure that the handling of personal data is carried out safely, reliably and protected from unauthorized or unauthorized access, collection, use, disclosure, deletion or destruction.
    b. Article 32 paragraph (1): The controller shall take adequate technical and organizational measures to ensure the security of the personal data processed, including protection against unauthorized or accidental access, disclosure, modification or deletion.
    c. Article 36 paragraph (1): Controllers and processors shall take measures to ensure that any person working for them who has access to personal data can only access such personal data for specified purposes.

Telemedicine providers to maintain the confidentiality of patients' personal data. This means that telemedicine providers should not disclose patients' personal data to third parties without the patient's consent.

Security

1. GDPR
    a. Article 32 GDPR requires controllers to take adequate technical and organizational measures to ensure the security of the personal data processed. These measures should be designed to prevent unauthorized access, use, disclosure or destruction of personal data.
    b. Article 33 GDPR requires controllers to report breaches of personal data security to the supervisor without unreasonable

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

delay and, where possible, within 72 hours of becoming aware of the breach.

2. PDP Act
   a. Article 26 paragraph (1) of the PDP Law requires controllers and processors to implement effective protection of personal data through the implementation of a series of engineering and organizational measures to ensure that the handling of personal data is carried out safely, reliably and protected from unauthorized or unauthorized access, collection, use, disclosure, deletion or destruction.
   b. Article 32 paragraph (1) of the PDP Law requires controllers to take adequate technical and organizational measures to ensure the security of personal data processed, including protection against unauthorized or accidental access, disclosure, modification or deletion.
   c. Article 36 paragraph (1) of the PDP Law requires controllers and processors to take steps to ensure that any person working for them who has access to personal data can only access such personal data for specified purposes.
   d. Article 52 paragraph (1) of the PDP Law gives the right to any person who suffers material or immaterial losses arising from a personal data breach to seek compensation from the controller or processor.

Telemedicine providers to implement security measures to protect patients' personal data. These security measures should be designed to prevent unauthorized access, use, disclosure, or destruction of patients' personal data.

Patient Rights

1. GDPR
   a. Article 15 GDPR gives data subjects the right to access information about their personal data processed by the controller. This information includes the purposes of processing, the categories of personal data processed, and the recipients of the personal data.
   b. Article 16 GDPR gives data subjects the right to request the controller to correct or delete their inaccurate or incomplete personal data.
   c. Article 17 GDPR gives data subjects the right to request the controller to delete their personal data in certain circumstances, such as if the personal data is no longer necessary for the purposes for which it was collected or if the data subject withdraws their consent.
   d. Article 21 GDPR gives data subjects the right to restrict the processing of their personal data in certain circumstances, such as if the data subject disputes the accuracy of their personal data or

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

if the data subject objects to the processing of their personal data for direct marketing purposes.

e. Article 77 GDPR gives data subjects the right to lodge a complaint with a data protection authority in the EU member state where the data subject lives or works or where a personal data breach is alleged to have occurred.

2. PDP Act
   a. Article 14 of the PDP Law gives the owner of personal data the right to access his personal data controlled by controllers and processors.
   b. Article 15 of the PDP Law gives the owner of personal data the right to request controllers and processors to correct his/her inaccurate or incomplete personal data.
   c. Article 16 of the PDP Law gives the personal data owner the right to request controllers and processors to delete their personal data in certain circumstances, such as if the personal data is no longer needed for the purpose for which it was collected or if the owner of the personal data withdraws their consent.
   d. Article 26 of the PDP Law gives personal data owners the right to restrict the processing of their personal data in certain circumstances, such as if personal data owners dispute the accuracy of their personal data or if personal data owners object to the processing of their personal data for direct marketing purposes.
   e. Article 72 of the PDP Act gives personal data owners the right to lodge a complaint with a data protection authority if they believe that their privacy rights have been violated.

Both Indonesia and the European Union give patients the right to access, correct, delete and restrict the use of their personal data. Patients also have the right to lodge a complaint with a data protection authority if they believe that their privacy rights have been violated

In addition to these similarities, GDPR also imposes some additional requirements for data protection in telemedicine, such as:

The GDPR requires telemedicine providers to take appropriate technical and organizational measures to protect personal data from unauthorized access, use, disclosure, modification, or destruction.

GDPR requires telemedicine providers to notify patients if there is a data breach that could pose a high risk to their privacy.

The PDP Law is still relatively new and it is unclear how it will be interpreted and enforced in the context of telemedicine. But overall, GDPR and the PDP Act have strong frameworks for protecting personal data in telemedicine. By following the principles set out in these regulations, telemedicine providers can help ensure that patient data is collected, used, and shared in a safe and secure manner.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

In addition to the above similarities, there are also some differences in personal data protection in telemedicine in Indonesia and in the European Union. One difference is that GDPR applies to all telemedicine organizations/providers that process EU resident data regardless of where the organization is located. On the other hand, the PDP Law only applies to telemedicine organizations/providers located in Indonesia. Next. The most significant difference is that the European Union has stricter personal data protection laws than Indonesia. The European Union's personal data protection law, called the General Data Protection Regulation (GDPR), has been in place since 2018. GDPR is the most comprehensive personal data protection law in the world and provides strong protection for individuals' personal data. GDPR requires telemedicine providers to comply with stricter requirements than personal data protection in Indonesia. While in Indonesia the law that regulates personal data is Law Number 14 of 2008 concerning Public Information Openness, but only applies to the government and other public bodies, Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) and Number 27 of 2022 concerning Personal Data Protection (PDP Law).

Another difference is that Indonesia does not have an independent personal data protection supervisory body while the European Union has an independent personal data protection supervisory body, called the European *Data Protection Board* (EDPB). EDPB is responsible for ensuring that companies comply with GDPR and protect individuals' personal data rights. EDPB has several powers, such as conducting investigations into violations of personal data protection law, sanctioning parties who violate personal data protection law, and issuing guidelines on the application of personal data protection law. So that the enforcement of personal data protection laws in Indonesia is still not effective, while in the European Union the enforcement of the law is more effective.

One of the most noticeable differences between GDPR and PDP Law is the way they handle approvals/permissions. Under GDPR, telemedicine providers must obtain consent from individuals before collecting and using their personal data for telemedicine services for telemedicine purposes. Consent must be given freely, specifically, uninformatively, and unambiguously. This means that patients should be able to give their consent to the use of their personal data for telemedicine services in a clear and understandable way, and they should be able to withdraw their consent at any time. The PDP Act does not have the same strict requirements for approval, and allows for less clear and informative and ambiguous consent.

In case of violation of personal data protection laws, both GDPR and PDP Law have different sanctions. The sanctions for violations of personal data protection laws in the European Union are more severe than the sanctions for violations of personal data protection laws in Indonesia. The GDPR allows penalties of fines of up to 4% of a company's annual global revenue or twenty million euros, whichever is greater, for serious violations. Law Number 27 of 2022 concerning Personal Data Protection only allows fines of up to five billion rupiah for serious violations.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

Below is a table summarizing the differences between personal data protection in telemedicine in Indonesia and in the European Union

Table 1. Differences between Personal Data Protection in Telemedicine in Indonesia and in the European Union

Feature	Indonesian	European Union
Coverage	Applies to all organizations that carry out personal processes of EU residents, regardless of their location	Only valid for organizations located in Indonesia
Governing laws	Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)	*General Data Protection Regulation* (GDPR)
Regulatory Board	Does not have a regulatory body	*European Data Protection Board* (EDPB)
Licensing	Less clear and informative and ambiguous	free, specific, informative, clear and unambiguous
Penalty	Lower fines (maximum 4 billion Rupiah)	Significant fines (up to £500,000 or 8 billion rupiah)

Protection of personal data in telemedicine is important to ensure that patients can access healthcare safely and their privacy is protected. Despite some differences, personal data protection on telemedicine in Indonesia and in the European Union as a whole is quite good. Both Indonesia and the European Union have strong personal data protection laws and are responsible for ensuring that companies comply with those laws. However, the European Union has more comprehensive data protection laws and has an independent data protection authority. This is because the European Union has a long history of protecting personal data, and they have developed personal data protection standards that are considered to be the strictest in the world.

Implementation of Personal Data Protection in Indonesia and GDPR in the European Union on Telemedicine

In Indonesia, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection in Electronic Systems and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) provide a legal basis for personal data protection. Especially in the Indonesian Personal Data Protection Law (PDP Law) which regulates the protection of personal data of Indonesian citizens aims to protect the personal data of Indonesian citizens from misuse by irresponsible parties. Telemedicine in Indonesia has been regulated in the Minister of Health Regulation no 20 of 2019 concerning the Implementation of Telemedicine Services Between Health Service Facilities. Telemedicine allows patients to

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

consult with doctors online through information and communication technology without having to come to the hospital.

The application of the PDP Law on telemedicine is essential to protect patients' personal data. Personal data of patients transmitted via telemedicine should be protected from misuse by irresponsible parties.

There are several things that can be done to apply the PDP Law to telemedicine, including:

1. Use adequate security technology to protect patients' personal data.
2. Conduct training for health workers involved in telemedicine on personal data protection.
3. Implement strict policies and procedures regarding personal data protection.

By applying the PDP Law to telemedicine, patients' personal data will be better protected from misuse. This will provide a sense of security for patients to use telemedicine services. The PDP Law provides a comprehensive legal framework for personal data protection in Indonesia, including in the context of telemedicine. Here are some of the applications of the PDP Law in telemedicine in Indonesia:

1. Consent and consent (Articles 12, 14, and 15 of the PDP Law): Telemedicine must obtain clear consent and consent from patients before collecting and processing their personal data. These consents and consents should be informational and specific, informing the purpose of the data collection, the types of data collected, and the rights of individuals regarding their personal data.
2. Data protection principles (Article 4 of the PDP Law): Telemedicine must comply with the principles of personal data protection stipulated in the PDP Law, such as the principles of fairness, transparency, specific objectives, data minimization, retention limitations, data integrity and security, and accountability.
3. Data security (Article 26 of PDP Law): Telemedicine needs to implement adequate technical and organizational security measures to protect patient data from unauthorized access, use, and disclosure. This includes physical and technical safeguards such as data encryption, use of appropriate access policies, and security certifications.
4. Data transfer (Article 32 of the PDP Law): If there is a transfer of patient data between telemedicine service providers, it is necessary to do so by ensuring that there are safeguards and mechanisms in place in accordance with the PDP Law. This can involve the use of contracts or data transfer agreements that protect patients' rights and privacy.
5. Individual rights (Articles 14, 15, 17 and 17 of the PDP Act): Telemedicine shall provide patients with individual rights guaranteed by the PDP Act, such as the right of access, rectification, deletion and refusal of processing of their personal data. Telemedicine should also have clear procedures in place to respond to these requests for individual rights.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

The implementation of the PDP Law in telemedicine is an important part of compliance with personal data protection standards and regulations in Indonesia. Telemedicine must maintain the privacy and security of patient data, as well as comply with the rules and requirements stipulated in the PDP Law to build trust and maintain integrity in the use of telemedicine technology in Indonesia.

EU regulations require all organizations, both public and private, that process the personal data of people in the EU to implement certain protective measures and disclose more information about what data they collect and how they will share it. It also provides more privacy protections for people and the data they may be able to provide to companies or government bodies. This EU regulation gives more control over the personal data of many people to those living in EU member states. This includes what information they provide, how that information is used, and who the data is shared with [15]. GDPR compliance enforced by the European Union through Data *Protection Directive* or Data Protection Directive. The directive provides a legal infrastructure that ensures consumers' rights to their personal data and ensures the punishment of any violations committed [16].

GDPR in the European Union has a number of implications on the adoption of telemedicine, such as:

1. Consent and Consent: Under GDPR, organizations must obtain consent from individuals before processing their personal data for most purposes. This means that organizations providing telemedicine services must obtain consent from patients before they can collect, use, or share their personal data.
2. Data transfer: The GDPR restricts the transfer of personal data outside the EU unless the receiving country has an adequate level of data protection. This means that organizations that provide telemedicine services to patients in the EU must ensure that their data is only transferred to countries deemed to have adequate data protection laws.
3. Security: The GDPR requires organizations to take appropriate technical and organizational measures to protect personal data. This means that organizations providing telemedicine services must ensure that their systems and processes are secure and they have appropriate safeguards in place to protect patient data.

Organizations providing telemedicine services in the European Union must comply with GDPR. Failure to comply with GDPR may result in fines. Here are some specific steps organizations can take to implement GDPR in telemedicine:

1. Conducting *a Data Protection Impact Assessment* (DPIA): DPIA is the process of identifying and assessing risks to individual privacy from

[15] Human Rights Watch, 'Peraturan Pelindungan Data Umum Uni Eropa', *Human Rights Watch*, 2018.
[16] (Princess, 2019)

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

data processing activities. Organizations providing telemedicine services should conduct DPIA to identify and assess risks to patient privacy from their data processing activities.

2. Appoint *a Data Protection Officer* (DPO): If an organization processes large amounts of personal data or if it performs certain types of data processing activities, it must appoint a DPO. The DPO is responsible for advising the organization on data protection compliance and for monitoring the organization's compliance with GDPR.
3. Implement appropriate technical and organizational measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction. This includes measures such as encryption, access control, and security awareness training.
4. Obtain consent from the patient before processing personal data. Consent must be free, specific, informed and unambiguous.
5. Only transfers of personal data to countries with adequate data protection laws. If an organization transfers personal data to a country that does not have adequate data protection laws, it must take additional measures to ensure the security of that data.

Learning Efforts on the Results of Comparative Laws Related to Personal Data Protection in Indonesia and GDPR in the European Union in Telemedicine

Based on the explanation above, researchers can see several things that can be learned both from personal data protection in Indonesia and GDPR in the European Union in the context of telemedicine:

1. Protection of Individual Rights: Through GDPR, the European Union places strong emphasis on protecting individual rights regarding personal data. Users have the right to access, correct, delete and restrict the use of their personal data. This gives individuals greater control over their personal data. In the context of telemedicine, the implementation of GDPR can be a good example for Indonesia in ensuring that individual rights related to personal data are respected and well protected.
2. Data Security Requirements: The GDPR provides strict requirements regarding the security of personal data. This includes protection against unauthorized access, loss, and destruction of data. In addition, GDPR encourages the adoption of appropriate technical and organizational security measures to protect personal data. In implementing telemedicine, it is important for Indonesia to pay attention to the security aspects of personal data by adopting the best practices set out in the GDPR.
3. Public Awareness and Education: The GDPR recognizes the importance of public awareness and education regarding personal data protection. The regulation encourages service providers to provide clear and transparent information about the use of personal data to individuals. This helps raise individuals' awareness of their rights regarding personal data and how to protect it. In Indonesia, similar

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

efforts need to be made to raise public awareness about personal data protection in the context of telemedicine.

Here are some points to consider in this analysis:

1. Public Awareness and Education
   a. Indonesia: Awareness about personal data protection in Indonesia is still in the developing stage. Although laws such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law already exist, public awareness of their rights regarding personal data still needs to be improved. Public education efforts are needed to provide a better understanding of the rights and risks associated with personal data in the context of telemedicine.
   b. European Union (GDPR): ** The European Union has a General Data Protection Regulation (GDPR), which regulates the protection of personal data very strictly. Awareness of personal data-related rights in the European Union is likely to be higher, and public education about GDPR has contributed to a better understanding of the importance of controlling personal information.
2. Legal Comparison
   a. Indonesia: The Personal Data Protection Law (PDP Law) in Indonesia has been in place since 2016. This law provides a framework for the protection of personal data, including medical data in telemedicine. However, its implementation still faces challenges, and many organizations have not fully complied with the requirements of the PDP Act.
   b. European Union (GDPR): GDPR is the regulation governing the protection of personal data in the European Union since 2018. The GDPR provides individuals with strong rights regarding the use and protection of their personal data. These include strict requirements regarding consent, the right to access data, and the right to be forgotten.
3. Telemedicine
   a. Indonesia: In the context of telemedicine in Indonesia, personal data protection is important as sensitive medical information is transmitted and accessed through digital platforms. Care is needed in managing patient medical data and ensuring data security in telemedicine services.
   b. European Union (GDPR): GDPR has significant implications in telemedicine in the European Union. Telemedicine service providers must ensure that medical data is processed in accordance with GDPR requirements, including lawful consent and strict data security.

The General Data Protection Regulation (GDPR) is a privacy and data protection regulation imposed by the European Union. The GDPR is a legal

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

framework that aims to protect the privacy rights of individuals and regulate the use of personal data across European Union member states. This regulation came into force on 25 May 2018 and replaced the previous Data Protection Directive [17].

The main goal of GDPR is to provide stronger protection of individuals' personal data and give individuals more control over their data. The GDPR covers a wide range of aspects, including the definition of personal data, companies' obligations in processing data, individuals' rights regarding their personal data, data security requirements, as well as regulations regarding data transfers outside the European Union.

Some key points in GDPR include:

a. Notification Requirements (Articles 13 and 14 GDPR): Organizations are required to provide clear and transparent notice to individuals about the use of their personal data.
b. Individual Rights (Articles 15, 16, 17, 18 and 20 GDPR): The GDPR gives individuals the right to access their personal data, correct errors, delete data, restrict data processing, and transfer data to other entities.
c. Legal Basis for Data Processing (Article 6 GDPR): The GDPR requires organizations to have a valid legal basis for processing an individual's personal data, such as voluntarily given consent or the need to perform a contract.
d. Data Protection Obligations (Articles 32 and 33 GDPR): The GDPR requires organizations to protect personal data by implementing appropriate security measures and reporting data breaches to appropriate authorities.
e. International Data Transfers (Articles 44 and 50 GDPR): The GDPR has specific rules regarding the transfer of personal data outside the territory of the European Union, which involves the requirement of adequate protection or the use of lawful data transfer mechanisms.

With the adoption of GDPR, the EU aims to create a uniform and consistent legal framework in protecting the privacy and security of personal data of individuals across the EU. GDPR also has a global impact as it affects organizations outside the European Union that process EU citizens' personal data. GDPR violations can result in significant fines for organizations that do not comply with the regulation.

By studying personal data protection in Indonesia and GDPR in the European Union, best practices and lessons can be identified that can be applied in developing a more effective legal and policy framework in protecting personal data in telemedicine in Indonesia. In facing existing challenges and needs, the implementation of GDPR can be a valuable source of inspiration and reference for Indonesia to improve personal data protection in telemedicine

[17] Dea Indria, Mohannad Alajlani, and Hamish S. F. Frase, 'Clinicians Perceptions of a Telemedicine System: A Mixed Method Study of Makassar City, Indonesia', *MC Medical Informatics and Decision Making*, 2020.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

D. Conclusions

Based on the results of the study, it can be concluded that personal data protection is important to maintain individual privacy and security. In Indonesia, personal data protection is regulated by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). While in the European Union, Personal Data Protection is regulated in the *General Data Protection Regulation* (GDPR) which regulates the collection and use of personal data by organizations. Some similarities in personal data protection both in telemedicine both in Indonesia and in the European Union are the same agreement requires telemedicine providers to obtain clear and explicit consent from patients. Telemedicine providers should not disclose patients' personal data to third parties without the patient's consent. Telemedicine providers to implement security measures to protect patients' personal data. Both Indonesia and the European Union give patients the right to access, correct, delete and restrict the use of their personal data.

Telemedicine in Indonesia has been regulated in the Minister of Health Regulation no 20 of 2019 concerning the Implementation of Telemedicine Services Between Health Service Facilities. Some applications of the PDP Law in telemedicine in Indonesia require obtaining clear consent and consent from patients before collecting and processing their personal data. Telemedicine must also comply with the personal data protection principles stipulated in the PDP Law. For data security, telemedicine needs to implement adequate technical and organizational security measures to protect patient data from unauthorized access, use, and disclosure. If there is a transfer of patient data between telemedicine service providers, it is necessary to do so by ensuring that there are safeguards and mechanisms in accordance with the PDP Law. Telemedicine should provide individual rights guaranteed by the PDP Act to patients. GDPR in the European Union has a number of implications on the implementation of telemedicine, such as: organizations must obtain consent from individuals before processing their personal data for most purposes. The GDPR restricts the transfer of personal data outside the EU unless the receiving country has an adequate level of data protection. This means that organizations that provide telemedicine services to patients in the EU must ensure that their data is only transferred to countries deemed to have adequate data protection laws. The GDPR requires organizations to take appropriate technical and organizational measures to protect personal data.

REFERENCES

Alfaridzi, Muhammad Rais, 'Analisis Framing Pemberitaan Kasus Kebocoran Data Pribadi Di Media Online (Studi Deskriptif Analisis Framing Model Robert N Entman Pemberitaan Terkait Kasus Kebocoran Data Pribadi Oleh Hacker Bjorka Di Tempo.Co Dan Kompas.Com Periode 22 Agustus – 18 Novem', *Universitas Sebelas Maret*, 2022

Arbella, Wan Indy Azka, 'Perbandingan Hukum Terhadap Perlindungan Data Pribadi Menurut Hukum Positif Indonesia Dan General Data Protection Regulation (GDPR) Uni Eropa', *Faculty of Law*, 2020

Council of the European Union, 'Interinstitutional File: 2012/0011 (COD)', 2015.June (2015), 201

Ferorelli, D., 'Medical Legal Aspects of Telemedicine in Italy: Application Fields, Professional Liability and Focus on Care Services During the COVID-19 Health Emergenc', *Italia : Journal of Primary Care and Community Health*, 11 (2020)

Ferorelli, D., L. Nardelli, L. Spagnolo, S. Corradi, M. Silvestre, F. Misceo, and others, 'Medical Legal Aspects of Telemedicine in Italy: Application Fields, Professional Liability and Focus on Care Services During the COVID-19 Health Emergency', *Journal of Primary Care and Community Health*, 11 (2020) <https://doi.org/10.1177/2150132720985055>

Indria, Dea, Mohannad Alajlani, and Hamish S. F. Frase, 'Clinicians Perceptions of a Telemedicine System: A Mixed Method Study of Makassar City, Indonesia', *MC Medical Informatics and Decision Making*, 2020

Iqbal, Muhamad, 'Privacy Policy | Global Climate Change', *STIA LAN*, 2022, p. 1

Lu, Hsiao Han, Wen Shan Lin, Christopher Raphael, and Miin Jye Wen, 'A Study Investigating User Adoptive Behavior and the Continuance Intention to Use Mobile Health Applications during the COVID-19 Pandemic Era: Evidence from the Telemedicine Applications Utilized in Indonesia', *Asia Pacific Management Review*, 28.1 (2023), 52–59 <https://doi.org/10.1016/j.apmrv.2022.02.002>

Nilamsari, Natalia, 'Memahami Studi Dokumen Dalam Penelitian Kualitatif', *Wacana*, 13.2 (2014), 177–81

Nugroho, Inaz Indra, Reza Pratiwi, and Salsabila Rahma Az Zahro, 'Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia', *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 1.2 (2021), 115–29 <https://doi.org/10.15294/ipmhi.v1i2.53698>

Putri, Annelis, 'GDPR, UU Perlindungan Data Uni Eropa', *CCM*, 2019

Ramadhani, Syafira Agata, Fakultas Hukum, and Universitas Brawijaya, 'Komparasi Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa', *Jurnal Hukum Lex Generalis*, 3.1 (2021), 73–84

Riyanto, Agus, 'Faktor-Faktor Yang Mempengaruhi Pelaksanaan Telemedicine (Systematic Review)', *Jurnal Manajemen Informasi Kesehatan Indonesia*, 9.2 (2021), 174 <https://doi.org/10.33560/jmiki.v9i2.337>

Suwadi, Pujiyono, 'Legal Comparison of the Use of Telemedicine between Indonesia and the United States', *International Journal of Human Rights in*

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 8, No. 2-December 2023

Healthcare, 2022

Watch, Human Rights, 'Peraturan Pelindungan Data Umum Uni Eropa', *Human Rights Watch*, 2018

Wijaya, Glenn, 'Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum', *Law Review*, XIX.3 (2020), 326–61

Zed, Mestika, *Metode Penelitian Kepustakaan* (Jakarta: Yayasan Obor Indonesia, 2003)