JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i4

The User's Position as Personal Data Controller in the Utilization of Electronic Systems in the Form of Messaging Applications in Review of Law Number 27 of 2022 concerning Personal Data Protection

Jonathan Matthew[1], Sinta Dewi Rosadi[2], Prita Amalia[3].
[1]Universitas Padjadjaran, West Java, Indonesia, jonathan20002@mail.unpad.ac.id.
[2]Universitas Padjadjaran, West Java, Indonesia, sinta@unpad.ac.id.
[3]Universitas Padjadjaran, West Java, Indonesia, prita.amalia@unpad.ac.id.

Corresponding Author: jonathan20002@mail.unpad.ac.id[1]

Abstract: In its development, privacy as the right to be let alone and privacy right has now been recognized and regulated more comprehensively and specifically in Law Number 27 of 2022 on Personal Data Protection (UU PDP), along with the increasing use of messaging applications as a digital communication medium by the public. In its general use, there is a flow of information, transmitted by and between users, which can be in the form of electronic documents and often simultaneously can contain personal data (privacy). In the transmission of information flows involving personal data, it can be seen that there are users who collect and process personal data (recipients of personal data), and there are users who are interlocutors, who also send personal data to recipients (senders of personal data). This research is conducted using normative juridical method and will discuss the position of the user of the messenger application as the controller of personal data in the utilization of the messenger application and its legal consequences according to the PDP Law. From the results of the research, it can be seen that the user of a messaging application who collects and processes personal data (recipient of personal data) of their interlocutor can act as a personal data controller in the context of the PDP Law, if the user manages personal data and determines the reasons (why and how) for the management. The legal consequences that arise include the regulatory provisions in the PDP Law, especially those relating to the obligations of personal data controllers, which apply to users in their position as personal data controllers, as well as legal liability in the event of unlawful acts against personal data.

Keyword: User, Personal Data Controller, Messaging Application, Position, PDP Law.

INTRODUCTION

Basically, the concept of personal data controller arises from efforts to provide protection for personal data as the privacy of an individual who in this case is the subject of personal data. Privacy can be interpreted as the right to be let alone, and is one of the human rights that is recognized and respected. This definition is based on the existence of a change in

meaning related to the nature and scope of protection of an individual's self and property, namely, if initially the law through the recognition of the right to life only provided a solution to physical intervention in life and property, now there needs to be recognition of the spiritual, emotional and intellectual nature of human beings (Warren & Brandeis, 1890).

In this regard, it can be said that the scope of protection of the right to life has now been expanded, namely the right to enjoy life which also includes the right to be let alone. Furthermore, along with developments, there is a new step in the context of guaranteeing privacy (the right to be let alone). Although initially legal, in order to respond to changes in social, political and economic aspects, it has taken the step of expanding the scope of protection to include personal and property so as to provide protection from physical violence (such as assault and so on) or from damage to reputation (through the concept of defamation and so on), but this can be said to be insufficient, because on the other hand there are also problems arising from the use of instant photography and from newspaper companies that then invade private life, which is related to the feelings of a person or individual (Bratman, 2002). This gives rise to the concept of privacy right, which can be defined as an individual's right to determine how personal information or data is used or shared by individuals or other parties, and privacy right also has a bearing on an individual's freedom (cannot be violated without clear reason).

Therefore, efforts to protect personal data as an individual's privacy are important, because of course the value of the losses suffered by individuals related to violations or misuse of personal data that constitutes that privacy will be greater than the value of physical losses, so that the aggrieved individual is then also entitled to compensation (Rosadi, 2017). In Indonesia itself, privacy (the right to be let alone) as a human right has been recognized in the constitution, which is found in Article 28G paragraph (1) of the 1945 Constitution (UUD 1945) which states that "Everyone has the right to protection of their personal privacy, family, honor, dignity and property under their control, and the right to feel safe and protected from the threat of fear of doing or not doing something that constitutes a human right".

Then, in its development, there are now regulations related to the protection of personal data as privacy in a more specific and comprehensive manner, as can be found in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law itself essentially has a scope that applies to the processing of personal data carried out by individuals, corporations, public bodies, and international organizations. In this regard, the PDP Law includes the concept of protection of privacy rights, which is regulated in relation to the rights of personal data subjects (rights of access, rights to rectification of data, rights to erasure of data, rights to object to automated processing and profiling, rights to transfer data, rights to object and rights to restrict processing). In addition, the PDP Law also regulates the obligations of controllers and processors of personal data, the types of personal data, and criminal sanctions for the misuse of personal data.

In everyday life, and also due to the rapid development of information and communication technology, it can be said that the use of messaging applications for communication activities by the public has become very common. According to the latest survey report, with the survey period being January 2024, it can be seen that the most common or most widely used messaging application by the public is WhatsApp which of all people aged 16 to 64 who use the internet, 90.9% of this group uses WhatsApp (Annur, 2024), followed by other digital social media that also have messaging or instant messaging features such as Instagram, Facebook, TikTok and so on.

This shows that messaging applications today (as digital social media) are basically a communication medium that is very close to people's lives. Messaging applications or instant messaging applications, which can also be said to be an electronic system in the form of software, can be defined as an application that provides real-time messaging services through the use of the internet (Yasa & Nugraha, 2024). Messaging applications enable text-based

communication between two or more users in real-time through the use of computers or mobile devices (Prabarini & Haswanto, 2021).

In its use as a communication medium, there is of course an information flow that is transmitted by and between users. The information that is transmitted by and between users in the use of messaging applications can be in the form of electronic documents containing text, sound, images, photos, and so on, and often simultaneously containing personal data (privacy). The tendency of users to transmit messages that often contain personal data in the use of messaging applications is basically related to the ease of use, speed, and supporting features that make it easy to communicate (Juniarmi, 2024; Pangaribuan et al., 2023). In particular, in a transmission involving the flow of personal data information, it can basically be seen that there are users who collect and process personal data, and there are also users who send personal data, namely the interlocutor. The user who collects and processes the personal data of the interlocutor can be identified as the recipient, while the sender is the interlocutor who sends electronic documents which often contain personal data.

Therefore, considering that the flow of information transmitted is between users, several questions may arise. These questions include, first, whether the user who collects and processes the personal data of the other party is then able to be the controller of personal data, namely the controller of the personal data of the other party that is collected and processed by the user in the flow of information (messages) transmitted in the use of the messaging application. In this regard, a question will arise again, namely what legal consequences may arise if the user is then positioned as a personal data controller.

For reference, there are several legal issues (facts) relating to the user's position as a personal data controller. Among them are, first, in the case of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent State Data Protection Center Schleswig-Holstein or ULD) against Wirtschaftsakademie Schleswig-Holstein GmbH (Schleswig-Holstein Business Academy) and Facebook Ireland, in which case The Grand Chamber of the ECJ (European Court of Justice) issued a decision regarding the interpretation of Article 2 letter d of the Data Protection Directive 95/46/EC (now found in Article 4 paragraph 7 of the GDPR which is also a provision related to the definition of "controller"), namely that the Schelswig-Holstein Business Academy, which manages a fan page on Facebook and is the subject of personal data (users) from Facebook as the controller of personal data, can ultimately also be referred to as the controller of personal data together with Facebook.

This is based on the reason that the Schelswig-Holstein Business Academy, as the manager of a fan page, influences the collection of Facebook data from visitors who visit the fan page, namely in terms of participation in determining the purpose and how to process the personal data of visitors to the fan page, considering that the statistical information received by the Schelswig-Holstein Business Academy through activities on its fan page on Facebook can be used for the purpose of managing the promotion of its activities, such as knowing the profile of visitors who like it so that it can provide more relevant content and so on.

Second, legal issues (facts) relating to the position of users as controllers of personal data can be found in the fact that in this era of rapid development of information and communication technology (the digital era), messaging applications as a communication medium (social media) are often used for various purposes, from those related to business interests to private or personal interests. For example, in the case of business interests, especially in messaging applications that have special features to support business needs. In their use, business actors often collect (receive) and process consumers' personal data, generally for the purposes of data collection, checkout, delivery of goods, and so on. In other words, there is the sending and receiving of personal data in the flow of information transmission between the two users of the messaging application (business actors and consumers), where business actors collect and process personal data sent by consumers in order to support the realization of their business.

Therefore, based on the above legal issues or facts, considering that there are now more specific and comprehensive regulations regarding the protection of personal data as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), especially the regulations governing personal data controllers in an effort to provide protection for personal data which constitutes privacy, then objective research can be carried out regarding the position of users as personal data controllers in the utilization of electronic systems in the form of messaging applications (including WhatsApp and other messaging applications as a digital social media).

In this regard, the focus of the research is to examine whether the regulatory provisions in the law related to personal data protection or the PDP Law in Indonesia allow a messaging application user to be categorized or positioned as a personal data controller, if the user collects and processes personal data in the flow of information (messages) transmitted by and between users, and then examines the legal consequences arising from this, so that in the end, it is hoped that this research will be able to better guarantee the realization of legal awareness in the future, which in turn can create legal certainty.

In relation to the description above, the main issues that will be discussed in this study are:

1. What makes a user who collects and processes personal data in the use of an electronic system in the form of a messaging application able to be a personal data controller under the PDP Law?
2. What are the legal consequences for users who collect and process personal data in the use of an electronic system in the form of a messaging application under the PDP Law?

METHOD

The approach used in this study is normative juridical with a statute approach. Through the normative juridical research method with a statutory approach, the research will be carried out by examining (studying) a problem, seen in terms of its legal rules, as well as examining library materials and so on (Soejono & Abdurahman, 2003). In other words, research will be carried out by examining (studying) a legal problem based on laws and regulations, supported by theories, concepts, principles or principles, as well as literature and other sources related to the research topic (the problem under study).

In this regard, there are several sources of literature that will be used, specifically in this case, namely Law Number 27 of 2022 concerning Personal Data Protection (PDP Law / UU PDP), the Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Personal Data Protection in Electronic Systems (Permenkominfo Nomor 20 Tahun 2016) and so on, then supported by theories and principles related to privacy, privacy rights, personal data protection, controllers and subjects of personal data, up to those related to messaging applications (instant messaging applications) and messaging application users; Literature related to research topics such as scientific journals and books on privacy, protection of privacy and others, to electronic literature.

RESULTS AND DISCUSSION

User Position as Personal Data Controller in the Utilization of Messaging Applications Based on Law Number 27 of 2022 concerning Personal Data Protection

As previously mentioned, in the use of messaging applications by users, there is often a transmission of messages (chat) containing personal data (sensitive data or information), sent in a chat room used by two types of users, namely the sender and the recipient. The message is sent by the sender and then utilized by the recipient, who often at the same time collects and processes personal data for specific purposes.

Referring to the PDP Law, there is basically no explicit regulation regarding the transfer of the position of an entity (in this case a user of an electronic messaging application) as a

controller of personal data. However, the criteria or elements of personal data controllers are formulated in the general provisions chapter of the PDP Law, although it is not a norm because it only serves to provide a definition, explain abbreviations, and reflect the intent and purpose. Thus, the elements of the definition of personal data controller in the PDP Law can be analyzed not as a norm, but to find out what the PDP Law means regarding personal data controllers.

The elements of personal data controllers in the PDP Law can be found in Article 1 number 4, which states that "Personal Data Controller is every person, public body, and international organization that acts individually or jointly in determining the purpose and controlling the processing of Personal Data".

First, it relates to the element of "every person". Based on Article 1 number 7, what is meant by every person is "a natural person or corporation", where a corporation is defined in Article 1 number 8 as "a collection of persons and/or organized wealth, whether incorporated or not". Basically, users of messaging applications, who collect and process personal data based on certain intentions and purposes, whether for purposes related to business interests or private interests, can generally be identified as corporations or individuals (natural person).

Furthermore, referring back to the other elements (criteria) of the personal data controller in Article 1 number 4 of the PDP Law, it is stated that the personal data controller "acts individually or jointly in determining the purpose and exercising control over the processing of Personal Data". This shows that the personal data controller in determining the purpose of processing and exercising control over processing can be done individually or jointly (consisting of two or more personal data controllers and so on).

Regarding the meaning of the elements of "determining the purpose" and "controlling the processing of Personal Data", it can basically be analyzed from several sources, namely literature, other laws and regulations, and regulatory provisions in the PDP Law itself.

1. The element of "determining the purpose"

Given that the PDP Law in its formation uses references from various regulatory concepts related to the protection of other personal data, especially those applicable in countries of the European Union, namely GDPR 2016 (Hukumonline, 2022), then to analyze the meaning of the element of "determining the purpose" can be seen from the meaning contained in a similar element in the definition of personal data controller, in this case as contained in the GDPR 2016. In the GDPR, an element similar to the element of "determining the purpose" in the definition of personal data controller in the PDP Law is found in Article 4 number 7 of the GDPR 2016, where the personal data controller in its definition contains the element of "determines the purposes and means".

If we refer to the guideline issued by the Europe Data Protection Board (EDPB) on the concept of personal data controllers and processors in the GDPR, then regarding the element of "determines the purposes and means" it can be interpreted that the personal data controller must determine the intent and purpose of the processing, namely relating to why and how of personal data processing (Europe Data Protection Board, 2020). In this case, a personal data controller is a party that determines why personal data processing is carried out, namely what the purpose is, what the processing is carried out for, and how the purpose will be achieved (what methods will be used, etc. to achieve the purpose).

This is also basically relevant to what is contained in the personal data protection guidelines (privacy) published by the OECD in 1980 and its amendment in 2013 before the formation of the GDPR, and has also become a reference in the formation of the PDP Law. In the OECD Privacy Guidelines, it is stated that one of the elements or criteria of a personal data controller is that the personal data controller is a party that is "competent to decide about the contents and use of data" (OECD, 2002, p. 36). From this element, it can be seen that the personal data controller has the authority to determine the content and use of data, which includes determining data processing activities (OECD, 2002), as well as determining the processing activity when related to the GDPR context as explained previously, it can also be

said to be related to determining the reason for processing personal data (including clarity of purpose, what it is done for and determining how to achieve the purpose of processing personal data).

Therefore, it can be concluded that the element of "determining the purpose" in the sense of personal data controller in the context of the PDP Law can be interpreted or defined as a personal data controller who determines the purpose of personal data processing, including determining why (for what reason personal data is processed) and how personal data will be processed (how to achieve the purpose of processing personal data (determining how personal data is processed)).

2. The element of "controlling the processing of Personal Data"

Regarding the meaning of the next element or criterion of the definition of Personal Data Controller in the general provisions of the PDP Law, it can basically be analyzed from several sources. First, in a book entitled Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional, a personal data controller is defined as an entity that manages personal data. The management in question is also defined as an activity, or series of activities, both through the use of automated and manual data processing technology, carried out in a structured manner and utilizing a data storage system, which is then carried out on personal data, including (but not limited to) the processing, collection, use, disclosure, dissemination and security of personal data (Rosadi, 2017).

If we then look at the formulation of the concept of personal data controller in the Academic Manuscript of the PDP Bill, we can find the same definition as in previous literature, although the Academic Manuscript of the PDP Bill still uses the term personal data manager. Personal data managers in the PDP Bill Academic Manuscript are defined as "persons, or legal entities, business entities, state administrative agencies, public bodies or other community organizations." (Naskah Akademik RUU PDP, p. 134).

Personal data managers then basically also manage personal data, which personal data management is also defined in the Academic Manuscript of the PDP Bill as an "activity or series of activities carried out on personal data, both by using automated and manual data processing tools, in a structured manner and using a data storage system, including but not limited to the collection, use, disclosure, dissemination and security of personal data." (Naskah Akademik RUU PDP, p. 136).

Based on the definitions in these literatures, it can be said that the element of "controlling the processing of personal data" in the definition of personal data controller in the PDP Law relates to the concept of personal data management. The management of personal data is also related to an activity, or a series of activities carried out on personal data, including (but not limited to) processing, collection, use, disclosure, dissemination and security. This management can be carried out both through the use of automated and manual data processing technology, carried out in a structured manner and utilizing a data storage system.

In other words, in the context of the PDP Law, the scope of management activities (management concept) by personal data controllers in "controlling the processing of Personal Data" basically includes (but is not limited to) collection, processing, use, disclosure, dissemination and security, which are carried out in a structured manner, both by utilizing automatic and manual data processing technology, as well as utilizing data storage systems.

This management concept is also reflected in the regulatory provisions of the PDP Law itself. First, referring to Article 16 of the PDP Law, it is regulated that the scope of personal data processing activities includes, among others, "acquisition and collection; processing and analysis; storage; repair and renewal; display, announcement, transfer, dissemination, or disclosure; and/or deletion or destruction".

Second, when referring to Chapter VI of the PDP Law regarding the Obligations of Personal Data Controllers and Personal Data Processors in the Processing of Personal Data, especially in the section on the Obligations of Personal Data Controllers (Articles 20 to 50),

there are many provisions that indicate that the PDP Law adheres to the concept of personal data management as contained in the definition of personal data controller (manager) in the literature described previously.

For example, Articles 35 to 40 of the PDP Law, which in the concept of personal data management relate to data security activities in the processing of personal data. In addition, Article 28 of the PDP Law, which in the concept of personal data management relates to the processing and use of personal data. Then also Article 20 of the PDP Law, which in the concept of personal data management relates to the collection (acquisition) of personal data. The reflection of the concept of personal data management in these provisions simultaneously demonstrates the intention of the element of "controlling the processing of personal data" in the sense of personal data controller according to the PDP Law.

In addition, the regulatory provisions related to the obligations of personal data controllers are also based on the principles of personal data protection in the PDP Law (Article 3) which describes the concept of personal data management. Principles such as protection, legal certainty, prudence, accountability and confidentiality basically describe the concept of personal data management. These principles relate to security guarantees for personal data in its processing, the legal basis for collecting and processing personal data, supervision of potential risks that may occur, accountability in the processing of personal data and so on.

Furthermore, there are also regulatory provisions in other laws and regulations that can be used as a reference in analyzing the meaning of the element "controlling the processing of Personal Data" in the definition of personal data controller in the PDP Law, especially in relation to the use of electronic systems such as messaging applications. If we look at the regulations in the Regulation of the Minister of Communication and Information Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems (Permenkominfo Nomor 20 Tahun 2016), there are several provisions that regulate users who obtain and process personal data in the utilization of electronic systems.

Article 27 in Regulation of the Minister of Communication and Information Technology Number 20 of 2016 states that users of electronic systems are obliged to "maintain the confidentiality of Personal Data obtained, collected, processed, and analyzed; use Personal Data only according to User needs; protect Personal Data and documents containing such Personal Data from misuse and be responsible for the Personal Data in their control, whether organizational control within their authority or individual control, in the event of misuse."

These regulatory provisions basically outline the concept of personal data management that must be carried out by users of electronic systems, including messaging applications, that control personal data.

The concept of personal data management according to these provisions is illustrated by requiring users who control personal data to implement a security system so that personal data can be protected and kept confidential, to implement a storage system as a form of accountability in data collection and processing, and so on. With the concept of personal data management in these provisions, it also describes the element of "controlling the processing of Personal Data" which is contained in the definition of personal data controller in the PDP Law.

Therefore, based on the explanation of the meaning of the elements of the definition of personal data controller in the general provisions of the PDP Law, it can then be concluded that:

a. The element of "determining the purpose" relates to determining why (for what reason personal data is processed) and how personal data will be processed (how to achieve the purpose of processing that personal data).

b. The element of "controlling the processing of Personal Data" relates to the concept of personal data management, which is an activity or series of activities, including (but not limited to) collection, processing, use, disclosure, dissemination and security, which are carried out in a structured manner, both utilizing automated and manual data processing technology, as well as utilizing a data storage system.

Based on this, it can also be concluded that users who utilize messaging applications to collect and process the personal data (recipient of personal data) of the other party can be referred to as personal data controllers in the context of the PDP Law if they manage personal data (fulfilling the element of "controlling the processing of personal data") and determine the reason (why and how) for the management of the personal data (fulfilling the element of "determining the purpose").

In this case too, it can be said that the user of a messaging application who is the controller of personal data is the controller of the personal data of the other party (the sender of the personal data) who is the subject of the personal data, because a user of a messaging application who is the controller of personal data will identify the other party who is the subject of the personal data through personal data that reflects the identity of the self, in accordance with specific intentions and purposes.

For example, if a user uses a messaging application for business purposes, it can be analyzed based on the elements of personal data controller that have been previously concluded to determine whether the user can then be referred to as a personal data controller in the context of the PDP Law.

First, it is necessary to know whether the user as a business actor will manage the personal data of his interlocutor who is a consumer, starting from collection, to other activities included in the concept of personal data management (processing, use, and so on).

At the same time, it is necessary to know whether the user as a business actor also states the intent and purpose of the personal data management, including the reason (why, what for) and an explanation of how to achieve the purpose of the personal data management that he or she carries out. With the fulfillment of these elements, the user of the messaging application as a business actor can be regarded as the controller of personal data, and the interlocutor (consumer) is the subject of personal data of the business actor.

Legal Consequences of Users as Personal Data Controllers in the Use of Messaging Applications Based on Law Number 27 of 2022 concerning Personal Data Protection

Legal consequences are basically defined as a consequence of legal actions, which are actions carried out with the aim of obtaining the desired result by the perpetrator and regulated by law (Sudjana, 2021). In other words, legal consequences are the desired result by the perpetrator of the legal action and regulated by law.

The elements of personal data controllers, as explained in the previous section, are basically related to personal data protection efforts. Personal data protection efforts are all efforts to protect personal data in the personal data processing chain to guarantee the constitutional rights of personal data subjects, and these efforts constitute a legal act (Budhijanto, 2023). In the case of users who, through the use of messaging applications, manage personal data and determine the intent and purpose of this management, in addition to being able to act as personal data controllers, it can also be said that they have committed a legal act. This is because the concept of personal data management (the element of "controlling the processing of Personal Data") accompanied by the determination of the intent and purpose of the management (the element of "determining the purpose") is a form of personal data protection effort which constitutes a legal act in the context of the PDP Law.

Because the concept of personal data management and the determination of the purpose of management are part of personal data protection as a legal act, it will then relate to a legal relationship. The legal relationship that arises from the management of personal data and the determination of the purpose and objectives of management as a legal act is that the regulatory provisions in the PDP Law are binding (the occurrence of a contract). Thus, the existence of these legal acts and relationships will result in legal consequences. Therefore, it is possible to analyze the legal consequences that arise if a messaging application user is the controller of personal data.

First, by managing personal data, accompanied by determining the intent and purpose of the management which then makes a messaging application user as the controller of personal data, it will result in legal consequences, namely the regulatory provisions in the PDP Law relating to the obligations of personal data controllers that apply to the personal data controllers concerned. These regulatory provisions include, among others:

a. Regarding the collection of personal data, it is reflected in Article 20 of the PDP Law which regulates the obligation of personal data controllers to have a basis for processing personal data. The basis for processing personal data according to Article 20 of the PDP Law includes:

a. Explicit legal consent from the Personal Data Subject for 1 (one) or several specific purposes that have been conveyed by the Personal Data Controller to the Personal Data Subject;
b. Fulfillment of contractual obligations in the event that the Personal Data Subject is one of the parties or to fulfill the request of the Personal Data Subject when entering into an agreement;
c. Fulfillment of legal obligations of the Personal Data Controller in accordance with statutory provisions;
d. Fulfilment of the protection of the vital interests of the Personal Data Subject;
e. Performance of duties in the context of public interest, public services, or the exercise of the authority of the Personal Data Controller based on statutory regulations; and/or
f. Fulfillment of other legitimate interests by taking into account the objectives (purposes), needs (necessity), and balance of interests of the Personal Data Controller and the rights of the Personal Data Subject.

From these provisions, it can be said that in the activity of "collecting" personal data as part of the concept (scope of activity) of personal data management, there needs to be an agreement between the subject of personal data and the controller (manager) of personal data. Basically, the agreement must be a legally valid agreement, based on Article 1320 of the Civil Code (it can also refer to Article 46 paragraph 2 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions if the contract is formed electronically).

With an agreement between the two parties, the management of personal data can be carried out by the personal data controller, in accordance with the predetermined objectives. This is in accordance with the provisions of Article 21 of the PDP Law, which states that if the processing (management) of personal data is based on consent, there must be information relating to the legality and purpose of the processing, the type and relevance of the personal data to be processed, the retention period of documents containing personal data, details relating to the information collected, the period of time for which the personal data will be processed and the rights of the data subject. Furthermore, personal data controllers must also pay attention to the provisions in Articles 22 to 24 of the PDP Law which also relate to agreements with personal data subjects.

b. Regarding processing, which also includes use, disclosure, dissemination and security, this is reflected in Articles 25 to 50 of the PDP Law. These articles include the obligations of personal data controllers in personal data processing activities, which include obligations in the case of processing the personal data of children and persons with disabilities, processing in a limited, specific, lawful and transparent manner, processing in accordance with the purpose, ensuring the accuracy, completeness and consistency of personal data, the obligation to update or correct errors or inaccuracies in personal data, the obligation to record personal data processing activities, to provide access to the subject of personal data, impact assessment in the case of high-risk personal data processing, certainty of personal data security (protection), up to that related to the destruction of personal data and the obligation to implement institutional orders. The obligations in the case of personal data processing by the personal data controller are also based on the principle of personal data protection in accordance with Article 16 paragraph (2) of the PDP Law.

c. Regarding the obligation of personal data controllers to appoint officials (officers) who carry out the function of personal data protection, as stated in Article 53 of the PDP Law. Personal data controllers in this case are obliged to appoint officials (officers) to carry out the function of personal data protection if there is personal data processing for the purposes of public services, the core activities of personal data controllers have the nature, scope and/or purpose that requires regular and systematic monitoring of personal data on a large scale, and the core activities of personal data controllers consist of large-scale personal data processing for personal data that is specific and/or related to criminal acts. In addition, based on Article 53 paragraphs (2) and (3), the officials (officers) implementing the personal data protection function can come from within and/or outside the personal data controller and are appointed based on professionalism, legal knowledge, personal data protection practices and the ability to fulfill their duties.

d. Regarding the obligations of personal data controllers in the case of transferring personal data outside the jurisdiction of the Republic of Indonesia. Referring to Article 56 paragraph (2), personal data controllers are obliged to ensure that the country of domicile of the personal data controller (and/or personal data processor) receiving the transfer of personal data has a level of personal data protection that is equivalent to or higher than that stipulated in the PDP Law. Furthermore, in paragraph (3), if the conditions in paragraph (2) are not met, the personal data controller must ensure that there is adequate and binding personal data protection. If the conditions in paragraphs (2) or (3) are not met, the personal data controller must obtain the consent of the personal data subject.

In the event of unlawful acts against personal data by the personal data controller, it is basically regulated in relation to the legal consequences in the PDP Law. First, referring to Article 57 of the PDP Law, perpetrators of unlawful acts against personal data as personal data controllers can be subject to administrative sanctions. Administrative sanctions can be given to personal data controllers if there is a violation of their obligations as covered in Articles 20, 21, 24, 25, and 56. These administrative sanctions can be in the form of written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data and/or administrative fines. Administrative sanctions are also imposed by institutions.

In addition, unlawful acts against personal data can also be subject to legal consequences in the form of criminal or civil liability. Basically, there are provisions that regulate prohibitions in the use of personal data, as stated in Articles 65 and 66 of the PDP Law. These prohibitions include prohibitions related to the acquisition or collection of personal data that does not belong with the intention of benefiting oneself or others that can cause harm to the subject of personal data (Article 65 paragraph (1)), prohibitions related to the disclosure of personal data that does not belong unlawfully (Article 65 paragraph (2)) and prohibitions related to the use of personal data that does not belong unlawfully (Article 65 paragraph (3)). Then there is also a related prohibition in the case of creating false personal data or falsifying personal data with the intention of benefiting oneself or others and causing harm to the subject of personal data (Article 66).

Based on these provisions, firstly, with regard to criminal liability, this is regulated in Articles 67 and 68 of the PDP Law. Broadly speaking, Article 67 regulates actions committed intentionally and against the law, violating the provisions of Article 65 paragraphs (1) to (3), which can be punished with imprisonment or a fine. Then Article 68 regulates the actions of anyone who deliberately falsifies personal data with the intention of benefiting themselves or others as stated in Article 66, and can also be punished with imprisonment or a fine.

Furthermore, with regard to civil liability, the personal data controller may be obliged to pay compensation to the personal data subject who has been harmed as a result of unlawful acts against personal data by the personal data controller. The obligation to pay compensation can originate from a type of default lawsuit (the personal data controller's failure to perform in accordance with the personal data processing agreement between the controller and the personal

data subject), or an unlawful act (the personal data controller commits an act that harms the personal data subject but is not based on any agreement, such as deliberately and unlawfully disclosing, using, changing, or acquiring personal data). Loss compensation is also basically regulated in the PDP Law, namely in Article 12 which states that "Personal Data Subjects have the right to sue and receive compensation for violations of the processing of Personal Data about themselves in accordance with statutory provisions".

Then, in the case of personal data management by the personal data controller of individuals based on the intent and purpose for household or personal interests, referring to Article 2 paragraph (2) of the PDP Law, the legal consequences for the personal data controller are that the provisions in the PDP Law (especially related to the obligations of the personal data controller) become invalid. Referring to the consideration of the Constitutional Court (MK) in case number 108/PUU-XX/2022 regarding the judicial review of Article 2 paragraph (2) of the PDP Law, it was stated that the processing of personal data carried out by individuals in household activities is processing carried out in the personal sphere (personal or private activities) so that it is non-commercial.

In other words, if the management of personal data is carried out by an individual for purposes that are not commercial or involving the public interest and are in the private sphere, such as in the case of kinship, family, and so on, then the provisions of the PDP Law, especially those relating to the principles, basis, and obligations in the processing of personal data, do not apply to the controller of the personal data concerned.

However, this does not mean that the protection of personal data, which is the privacy of the personal data subject, is also waived. If, then, from the management of personal data by the personal data controller for private purposes, there is misuse of personal data in the form of unlawful use, disclosure, alteration, and so on, the aggrieved personal data subject can still hold the perpetrator accountable.

CONCLUSION

The PDP Law basically does not yet contain regulatory provisions (norms) that explicitly regulate the transfer of the position of an entity, especially messaging application users, as personal data controllers. The criteria related to personal data controllers are contained in the chapter on general provisions of the PDP Law, which is not a norm, but only a definition.

However, from an analysis of the criteria for personal data controllers in the general provisions of the PDP Law based on literature, the provisions of the PDP Law and other relevant laws and regulations, it can be seen that the term "personal data controller" in the PDP Law refers to an entity that manages personal data and determines the purpose or reason (why and how) of the management of personal data. Thus, users of a messaging application whose purpose is to collect and process the personal data (recipient of personal data) of the other party can be considered as personal data controllers if they manage the personal data (fulfill the element of controlling the processing of personal data) and determine the reason (why and how) for the management of the personal data (fulfill the element of "determining the purpose").

There are several legal consequences arising from the position of a messaging application user as a personal data controller. First, the regulatory provisions in the PDP Law, especially those relating to the obligations of personal data controllers, apply to the user concerned (including those relating to the basis for processing personal data and the obligations in carrying out the processing).

Then, in the event of unlawful acts against personal data, the legal consequences that arise include, among others, that the perpetrator of the unlawful act against personal data can be subject to administrative sanctions. Administrative sanctions can be imposed by the agency on the personal data controller if there is a violation of his or her obligations.

In addition, the perpetrator of unlawful acts against personal data can also be held criminally or civilly liable by the aggrieved victim based on applicable legal provisions.

Furthermore, in the case of personal data management by users as controllers of personal data of individuals based on the intent and purpose for household or personal interests, the legal consequences for the personal data controller are that the provisions in the PDP Law (especially related to the obligations of personal data controllers) become invalid. Household or personal interests mean that the management of personal data is carried out by individuals with non-commercial purposes or intentions, not involving the public interest and in the private sphere. However, if the management of personal data in the private (household) sphere involves the misuse of personal data (unlawful acts), the aggrieved personal data subject can still hold the perpetrator accountable.

Considering that there are still phenomena of unlawful acts in the form of misuse of personal data in society, especially through the use of messaging applications, it is basically necessary to educate or socialize the community regarding the urgency of personal data protection in everyday life.

These phenomena of unlawful acts show that the level of public legal awareness of the importance of personal data protection is still low, so that the abuse of personal data, especially through the use of messaging applications, is still common. In this case, the public is also often unaware of their legal position in the context of personal data protection, as well as the legal consequences that can arise if personal data is misused. Therefore, it is important to carry out outreach or socialization efforts on personal data protection to the community, including providing an understanding of how they, as users of a messaging application, can be positioned as personal data controllers in its use, as well as the legal consequences that arise in accordance with what is intended and has been formulated in the PDP Law.

In addition, the existence of a personal data protection agency is also important. This is due, among other things, to the potential for unlawful acts against personal data by personal data controllers, so the existence of an agency is important for victims who have been harmed, especially considering some of the main functions of a personal data protection agency, which include formulating and enacting personal data protection policies, overseeing the implementation of personal data protection, enforcing administrative law, and facilitating dispute resolution. With the existence of a personal data protection agency, victims have the option of lodging a complaint (reporting) in the event of misuse of their personal data, so that law enforcement can then be carried out and provide legal certainty and justice for the victims.

REFERENCE

Annur, C. M. (2024). Ini media sosial paling banyak digunakan di Indonesia awal 2024. Databoks. https://databoks.katadata.co.id/datapublish/2024/03/01/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024

Bratman, B. E. (2002). Brandeis and Warren's The Right to Privacy and The Birth of The Right to Privacy. Tennessee Law Review, 69, 630.

Budhijanto, D. (2023). Hukum Pelindungan Data Pribadi di Indonesia, Cyberlaw & Cybersecurity (Cetakan Kesatu). Bandung: PT. Refika Aditama.

Constitutional Court of Indonesia. (2022). Decision No. 108/PUU-XX/2022.

David, B. (2000). Privacy & Human Rights 2000: An International Survey of Privacy Laws and Developments. Privacy International dan Electronic Privacy Information Center.

Europe Data Protection Board. (2020). Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Europe Data Protection Board.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

Hukumonline. (2022). Babak baru dan implementasi UU PDP bagi pelaku usaha dan masyarakat. Hukumonline. https://www.hukumonline.com/berita/a/babak-baru-dan-implementasi-uu-pdp-bagi-pelaku-usaha-dan-masyarakat-lt6390028f01b21?page=all

Juniarmi, I. (2024). Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Enkripsi

End-to-End. Technologia Journal, 1(2), 30–31.
Law Number 27 of 2022 concerning Personal Data Protection.
Naskah Akademik Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP).
OECD. (2002). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD. https://doi.org/10.1787/9789264196391-en
Pangaribuan, T., et al. (2023). Kesadaran Keamanan dan Privasi Data Pengguna Whatsapp (Studi Kasus di Provinsi Jawa Barat). Jurnal Studi Komunikasi dan Media, 27(1), 93–108. https://doi.org/10.17933/jskm.2023.5129
Prabarini, M. A., & Haswanto, N. (2021). Kajian User Interface Aplikasi Pesan Instan Berbasis Mobile.
Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Personal Data Protection in Electronic Systems.
Rosadi, S. D. (2017). Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional.
Rosadi, S. D. (2017). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit dikaitkan dengan Undang-Undang No 11 Tahun 2008 tentang ITE dan Peraturan Bank Indonesia No 7/6/PBI/2005. Sosiohumaniora, 19(3), 208. https://doi.org/10.24198/sosiohumaniora.v19i3.11380
Sudjana. (2021). Makna Mediasi dalam Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta. Veritas et Justitia, 7(1), 91–114. https://doi.org/10.25123/vej.v7i1.3716
Soejono, & Abdurahman, H. (2003). Metode Penelitian Hukum. Jakarta: Rineka Cipta.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193.
Yasa, R. N., & Nugraha, A. C. F. (2024). Perbandingan Keamanan Aplikasi Pesan Instan Android Menggunakan MobSF (Mobile Security Framework) Berdasarkan Beberapa Standar. Info Kripto, 18(1), 9–14. https://doi.org/10.56706/ik.v18i1.88.