Barelang Journal of Legal Studies
Volume 1 Issue 1 (March 2023), PP. 31-55
ISSN (Online): -
Published by Universitas Internasional Batam, Indonesia

Failing to Protect Personal Data: Key Aspects of Electronic System Operators' Agreements

Julienna Hartono[1], Angelica Milano[2], Xavier Nugraha[3*], Stefania Arshanty Felicia[4]
*Corresponding Author

Received: 28-1-2023
Revised: 20-2-2023
Accepted: 31-3-2023
Published: 25-5-2023

Citation:
Hartono, J., Milano, A., Nugraha, X., & Felicia, S. A. (2023). Failing to Protect Personal Data: Key Aspects of Electronic System Operators' Agreements. *Barelang Journal of Legal Studies*, 1(1), 31-55.

ABSTRACT

The rise of information technology has led to an increase in personal data processing by Electronic System Operators (ESOs). To ensure compliance with personal data protection principles, a personal data processing agreement is necessary for the involved parties: the controllers and processors of personal data. This agreement governs the ESO's liability in the event of a data protection failure. Regulating this aspect within a legal framework provides legal certainty and safeguards for all parties involved. By comparing personal data protection laws in Indonesia and the European Union, this article examines two key issues: the aspects of personal data processing agreements and the liability of ESOs in the event of data protection failure. The goal is to analyze the legal similarities and differences surrounding personal data protection.

Keywords: Electronic System Operators, Data Protection, Personal Data Processing Agreement
DOI: http://dx.doi.org/10.37253/barjoules.v1i1.7412

[1] Faculty of Law, Universitas Airlangga, Indonesia, hartonojulienna@yahoo.co.id
[2] Faculty of Law, Universitas Airlangga, Indonesia, angelica.milano.aryani-2021@fh.unair.ac.id
[3] Faculty of Law, Universitas Airlangga, Indonesia, nugrahaxavier72@gmail.com
[4] Faculty of Law, Vrije Universiteit Amsterdam, Netherlands, stefania.arshanty.felicia@gmail.com

INTRODUCTION

As technology develops in the digital era, various transaction activities begin to be carried out using electronic media in cyberspace (Tektona, 2023; Saputra, Rachim & Taniady, 2023; Disemadi, 2021). This change requires a legal framework that regulates legal actions carried out in cyberspace. Therefore, the Government of Indonesia issued Law No. 11 of 2008 on the Electronic Information and Transaction which was later amended by Law No. 19 of 2016 on the Amendments to Law No. 11 of 2008 on the Information and Electronic Transactions (hereinafter referred to as the ITE Law). Along with its implementing regulations and Law No. 27 of 2022 of Personal Data Protection (hereinafter referred to as the PDP Law). Based on Article 1 paragraph 2 of the ITE Law jo. Article 1 point 2 of Government Regulation No. 71 of 2019 on the Implementation of Electronic Information and Transaction (hereinafter referred to as PP PSTE), electronic transactions are "legal actions carried out using computers, computer networks, and/or other electronic media". Every time users make an electronic transaction; users are required to enter personal data (Baiq, 2021). For example, a seller who wants to offer his product through an e-commerce application or someone who wants to invest some money through securities application, both have to registering and inputting personal data such as self-identity, home address, bank account number, ID Card (KTP), taxpayer identification number (NPWP), etc (Kurniawan, Nugraha, Abrianto & Ramadhanti, 2020).

The definition of personal based on Article 1 paragraph 1 PDP Law are any data concerning a person, whether identified or who may be identified independently or combined with other information, either directly or indirectly, through an electronic or non-electronic system. Personal data entered by the user is then collected and processed by the relevant platform. In the ITE Law and its implementing regulations, parties who process personal data are called Electronic System Operators (hereinafter referred to as ESO). According to Article 14 paragraph (2) Government Regulation No. 71 of 2019 regarding the Implementation of Electronic Systems and Transactions (hereinafter referred to as PP PSTE) jo. Article 16 paragraph (1) of the PDP Law, data processing activities include: a) acquisition and collection, b) processing and analysis, c) storage, d) repair and update, e) appearance, announcement, transfer, dissemination, or disclosure and f) deletion or destruction.

From the description above, the processing of personal data is a complex event, starting from the collection, processing, to disclosure or destruction of data (Putra, Budiartha & Ujianti, 2023). In each stage of data processing, ESO is required to apply the principles of personal data protection (Muhammad & Nugroho, 2021), as mandated by Article 14 paragraph (1) PP PSTE jo. Article 16 paragraph (2) PDP Law includes: personal data is confidential in accordance with approval, responsibility for personal data in control, guarantees of integrity, accuracy, validity and updating of personal data, and others. The same thing regulated in Article 28 letter b PERMENKOMINFO PDP which regulates ESO obligations, one of which is maintaining the truth, validity, confidentiality, accuracy, and relevance as well as suitability for the purpose of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, disseminating, and destroying personal data.

If the ESO fails to apply the principles of personal data protection, then the ESO must be held responsible, this is explicitly regulated in Article 15 ITE Law jo. Article 3 paragraph (2) PP PSTE: "Electronic System Operators are responsible for the operation of their Electronic Systems." The responsibility of ESO as a Personal Data Controller in Article 47 PDP Law is also obliged to be responsible for processing Personal Data and show responsibility in the obligation to implement the principles of Personal Data Protection. The responsibilities of legal subjects themselves are divided into three, namely criminal, civil, and administrative responsibilities. As for what will be discussed in this study is the civil liability of ESO which according to law is known as liability. ESO that fails to protect personal data must be held accountable, as stated in article 39 paragraph (1) ITE Law: "Civil lawsuits are carried out in accordance with the provisions of the Laws and Regulations." This is also reaffirmed as one of the rights of Personal Data Subjects in Article 12 paragraph (1) PDP Law: "Personal Data Subjects have the right to sue and receive compensation for violations of processing Personal Data about themselves in accordance with statutory provisions."

Country that also has regulations related to personal data protection is the European Union, namely Regulation (EU) 2016/679 on General Data Protection Regulation (hereinafter referred to as GDPR). Based on Article 1 paragraph (2) GDPR, the European Union recognizes the protection of personal data as a fundamental right (Brkan, 2019). The principles that must be applied in data processing include: 1) legitimacy, fairness and transparency, b) purpose restrictions, c) data

minimization, d) accuracy, e) retention restrictions, f) integrity and confidentiality, and g) accountability (vide. Article 5 GDPR) (Tsamara, 2021). Just like the ITE Law and the PDP Law, the GDPR also stipulates that the party processing personal data will be held accountable if they violate the principles of personal data protection. Article 82 paragraph (2) GDPR stipulates that "Any controller involved in processing shall be liable for the damage caused by processing which infringes this regulation. A processor shall be liable for the damage ….".

It is possible for two or more ESOs to cooperate in processing personal data. In other words, data processing is carried out by more than one ESO (European Data Protection Board, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, EDPB, 2021). For example, company A is tasked with collecting data, but it is company B that processes the data. In this case, the ITE Law and its implementing regulations recognize external parties other than ESO, including Electronic System Users and Electronic Agents. (*vide*. Article 1 point 7 PERMENKOMINFO PDP jo. Article 1 point 3 PP PSTE). However, the regulation of legal relations between the parties is minimal. Slightly different from the provisions in the ITE Law, the PDP Law recognizes two types of data processing parties as controllers and processors of personal data, in which the legal relationship between the two is regulated in Article 51 PDP Law, namely: in the case of a Personal Data Controller appointing a Personal Data Processor it is obligatory to process Personal Data based on the order of the Personal Data Controller, the Personal Data Processing referred to in paragraph (1) is included in the responsibility of the Personal Data Controller, the Personal Data Processor may involve the Personal Data Processor in terms of processing Personal Data, the Personal Data Processor must obtain written approval from the Personal Data Controller before involve other Personal Data Processors as referred to in paragraph (4), and in the event that the Personal Data Processor performs the processing Personal Data outside the orders and purposes set by the Personal Data Controller, the processing of Personal Data is the responsibility of the Personal Data Processor. This is similar to the GDPR, there are two types of parties in the processing of personal data, namely controllers and processors, where the legal relationship between the two has been regulated in the GDPR, namely the obligation to sign a personal data processing agreement in writing. Differences in rights and obligations between controllers and processors have legal consequences in terms of liability if there is a failure

in protecting personal data (European Data Protection Board, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, EDPB, 2021).

From the description of the legal issues, there is a difference between Indonesia and the European Union regarding aspects of personal data processing agreements and ESO liability in the event of a personal data protection failure. It appears that both Indonesia and the European Union have legal regulations regarding the processing of personal data. Therefore, there are two formulations of the problem in this writing, **first**, aspects of personal data processing agreements in Indonesia and the European Union, **second**, aspects of the liability of Electronic System Operators in the failure of personal data protection in Indonesia and the European Union. This paper aims to analyze the similarities and differences in the legal aspects of personal data processing agreements and ESO liability between Indonesia and the European Union.

There are several articles that have previously discussed topics similar to this writing, namely a) The article written by Maldi Omar Muhammad and Lucky Dafira Nugroho entitled "Legal Protection of E-Commerce Application Users Affected by Personal Data Leaks". The article basically focuses on the leakage of e-commerce application personal data prior to the enactment of the PDP Law. Compared to that article, this article contains an explanation with a wider scope of aspects of the agreement and liability in the event of a personal data protection failure due to an Electronic System Operator; and b) The article written by Igor Inácio and Victoria da Silveira e Silva at SSRN (Nova School of Law) entitled "The Liability of Data Controller and Data Processor". The article basically discusses aspects of the liability of data controllers and data processors in the GDPR. When compared with these articles, this article provides a comparative explanation of EU law (GDPR) and Indonesian law with a particular focus on civil aspects through agreements and liability.

METHOD

This writing is legal research or normative juridical legal research, with the type of legal research being doctrinal research (Disemadi, 2022). Legal research doctrinal research is research that provides systematic explanation of the rules governing certain legal categories, analyzes the relationships between rules, explains areas of difficulty, and predicts future developments. In other words, the author will analyze the relevant regulations to obtain answers to the problem

formulation. In answering legal issues, the author uses three approaches to the problem, to wit the statute approach, the conceptual approach, and the comparative approach. The legal materials to be collected in this paper are primary and secondary legal materials. The primary legal materials are: a) *Staatsblad* No. 23 of 1847 concerning *Burgerlijk Wetboek Voor Indonesie*; b) Law No. 11 of 2008 of Electronic Information and Transaction; c) Law No. 19 of 2016 of Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions; d) Government Regulation No. 71 of 2019 of Implementation of Electronic Information and Transactions; e) Regulation of the Minister of Communication and Informatics No. 20 of 2016 of Protection of Personal Data in Electronic Systems; and f) Regulation (EU) 2016/679 on General Data Protection Regulation. The secondary legal material used by the author is in the form of legal opinions which are used to complement the primary legal sources. The legal materials above were obtained through library research. Primary legal materials were obtained from the website of the State Gazette and the website of the Legal Documentation and Information Network (JDIH) of various related agencies. Secondary legal materials in the form of legal opinions are obtained from books and articles sourced from online media, journals, and legal thesis, as well as other reading materials deemed relevant. Legal materials both primary and secondary that the author has obtained, will then be sorted based on the formulation of the problem that has been prepared by the author, to then be analyzed using legal research methods, one of which is deductive reasoning, namely drawing conclusions from general premises (laws and regulations) and special premises (events or legal actions).

DISCUSSION AND ANALYSIS

Data Protection: A Comparative Look at Indonesia and the EU

Given the complex process, often the processing of personal data involves more than one party (Nursiyono & Huda, 2023). To make it easier to understand, an illustration will be made a developer uses outsource marketing to market his new project in the form of an apartment. The company implements an hourly wage payment system, besides that marketers will also get bonuses if they succeed in getting buyers. The developer and the outsourcing company use a check-clock application that can be accessed through gadgets to record the working hours of their workers, then the recorded data is sent to the developer and the outsourcing company. Data on

working hours and personal data of workers are submitted and processed by company X to determine wages and bonuses. Company X is also assigned to pay wages to workers. Of course, in this case, the parties need to sign an agreement that regulates the rights and obligations of each party in processing personal data. This agreement is called the personal data processing agreement (GDPR Register, 2022).

Personal Data Processing Agreement According to Indonesian law

The ITE Law, its implementing regulations, and the PDP Law allow the processing of personal data by more than one party, this can be proven by the following article descriptions: Article 1 number 6a ITE Law mentioned "Electronic System Operator is every person, state administrator, Business Entity, and the public who provide, manage, and/or operate Electronic Systems **individually or jointly** to Electronic System Users for their own needs and/or the needs of other parties". Article 36 paragraph (1) PP PSTE "Electronic System Operators can operate their Electronic Systems **themselves** or **through** Electronic Agents". Article 21 paragraph (2) PERMENKOMINFO PDP mentioned "Display, announce, send, disseminate, and/or open access to Personal Data in the Electronic System as referred to in paragraph (1) including those carried out **between Electronic System Operators, between Electronic System Operators and Users, or between Users".** Article 1 number 4 of the PDP Law mentioned "Personal Data Controller is any person, public body and international organization acting **individually or jointly** in determining the purpose and exercising control over the processing of Personal Data". Based on Indonesian law, the personal data processing agreement is an anonymous agreement, namely an agreement that is not specifically regulated in BW (Bakarbessy & Anand, 2018). Legal subjects are allowed to make other agreements other than those stipulated in the BW based on the principle of freedom of contract as implicitly regulated in Article 1338 paragraph (1) BW, namely "all agreements made legally apply as laws for those who make them".

The ITE Law and its implementing regulations recognize several parties in the processing of personal data, including: **Electronic System Operator (ESO)**. As described above, ESO is a party that provides and manages electronic systems. The electronic system itself is a series of electronic devices and procedures that function to prepare, collect, process, store, display, announce, send and/or disseminate Electronic Information (vide. Article 1 number 5 ITE Law). One of the activities carried out by ESO is the processing of personal data, as stated in Article 14

PP PSTE. Related to the illustration at the beginning of the sub-chapter, company X is the ESO which is tasked with processing data on workers' working hours and making wage payments to these workers. In this case, of course Company X stores employee personal data, including employee identity and bank account numbers. **Electronic System Users**. Based on Article 1 number 7 PERMENKOMINFO PDP, Electronic System Users are people, state administrators, business entities, and the public who utilize goods, services, facilities, or information provided by ESO. Users of electronic systems need to be distinguished from owners of personal data, both are different legal concepts, as PERMENKOMINFO distinguishes the two. Based on Article 1 number 3 PERMENKOMINFO PDP, the owner of personal data is an individual to whom certain individual data is attached. Electronic System Users are also parties who process personal data, because in certain cases, Electronic System Users also process personal data, this is as stipulated in Article 27 PERMENKOMINFO PDP, where one of the obligations of electronic users is "to maintain the confidentiality of the Personal Data **obtained, collected, processed, and analyzed**. The activities of obtaining, collecting, processing, and analyzing are also stages in the processing of personal data. If related to the illustration, developers and outsourcing companies are Electronic System Users. **Electronic Agent**. Based on Article 1 number 8 of the ITE Law jo. Article 1 number 3 PP PSTE "Electronic Agent is a device of an Electronic System that is made to perform an action on certain Electronic Information automatically held by Persons." Electronic Agents can take the form of visual, audio, electronic data, and other forms (vide. Article 36 paragraph (4) PP PSTE). As for the explanation of the article, an example of a visual Electronic Agent is a graphical display of a website, audio for example telemarketing, and data electronics such as electronic data capture (EDC), radio frequency recognition (RFI), and barcode recognition. It should be underlined that one of the characteristics of an electronic agent is to process data automatically (Kadly, Rosadi & Gultom, 2021). But however automated, its existence is still part of the processing of personal data. If related to the illustration, the check-clock application is an electronic agent because it records worker data in the form of identity and working hours automatically.

Regarding the contents of the personal data processing agreement on Article 38 paragraph (2) PP PSTE, where the agreement on the use of electronic agents for more than one ESO interest must contain: a) rights and obligations, b) responsibilities, c) complaint mechanism and dispute

resolution, d) timeframe, e) fees, f) scope of services, g) choice of law. It should be noted that the above provisions only apply to the use of electronic agents for more than one ESO purpose. Although the above legal norms can be used as a reference in determining the contents of the data transfer agreement, the contents of the agreement mentioned above appear to be very simple when compared to the complex stages of processing personal data. Therefore, further arrangements regarding the contents of the personal data transfer agreement are once again left to the agreement of the parties based on the principle of freedom of contract. However, freedom in deciding the contents of this agreement still has limitations, as stipulated in Article 1337 BW, that the agreement (or its clauses) will be null and void if it violates the provisions of laws and regulations, decency, and general welfare (Anand, 2011). As for the provisions of the legislation that has been set the obligations of the parties in the personal data processing agreement include:

Article 28 PERMENKOMINFO PDP mentioned "Every Electronic System Operator must: a) Certify the Electronic System that it manages in accordance with the provisions of laws and regulations; b) Maintain truth, validity, confidentiality, accuracy and relevance as well as suitability for the purpose of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, disseminating and destroying Personal Data; c) Notify in writing to the Personal Data Owner if there is a failure to protect confidential Personal Data in the Electronic System that it manages, with the notification conditions as follows: Has internal rules related to the protection of Personal Data in accordance with the provisions of laws and regulations; Provide audit trail records of all Electronic System operation activities that it manages; Provide options to the Personal Data Owner regarding the Personal Data that they manage can/or cannot be used and/or displayed by/to third parties on the Approval as long as it is still related to the purpose of obtaining and collecting Personal Data; Provide access or opportunity to Personal Data Owners to change or update their Personal Data without disrupting the Personal Data management system, unless otherwise stipulated by the provisions of laws and regulations; Destroy Personal Data in accordance with the provisions in this Ministerial Regulation or the provisions of laws and regulations other invitations specifically stipulated in each Sector Supervisory and Regulatory Agency for that purpose; and Provide a contact person who is easily contacted by the Personal Data Owner regarding the management of his Personal Data".

Article 27 PERMENKOMINFO PDP mentioned "Required user to: Maintain the confidentiality of the Personal Data obtained, collected, processed and analyzed; Use Personal Data only according to User needs; Protect the Personal Data and the documents containing the Personal Data from misuse; and Is responsible for the Personal Data contained in his control, both organizational control under his authority and individuals, in the event of an act of misuse".

Article 40 paragraph (1) PP PSTE mentioned "Electronic Agent Operators must: Carry out identity authentication tests and check the authorization of Electronic System Users who carry out Electronic Transactions; Have and implement policies and procedures to take action if there is a proven indication of data theft; Ensuring control of authorization and access rights to Electronic Transaction systems, databases and applications; Develop and implement methods and procedures to protect and/or keep confidential the integrity of data, records, and information related to Electronic Transactions; Have and implement standards and control over the use and protection of data if the service provider has access to the data; Have a business continuity plan including an effective contingency plan to ensure the availability of Electronic Transaction systems and services on an ongoing basis; and Have procedures for handling unexpected events that are fast and appropriate to reduce the impact of an incident, fraud, and Electronic System failure.

From the description above, it can be concluded that the ITE Law and its implementing regulations recognize 3 parties that process personal data, namely ESO, Electronic System Users and Electronic Agents. The legal relationship between them is regulated in a personal data processing agreement which is still strong with the principle of freedom of contract. Thus, the parties can agree on their respective rights and obligations as long as they do not conflict with matters that have been regulated in laws and regulations.

Meanwhile, according to the PDP Law, there are 2 different parties in the processing of personal data, namely: **Personal Data Controller**. As described in Article 1 number 4 PDP Law, a Personal Data Controller is a party that either individually or jointly determines the objectives and exercises control over the processing of Personal Data. The main activity carried out by the Personal Data Controller is to determine the purpose and take control in the processing of personal data. If related to the illustration above, the developer and the outsourced company act as personal data controllers because they jointly determine the purpose of using the personal data.

Personal Data Processors. Based on Article 1 number 5 PDP Law, Personal Data Processors are any person, public body and international organization that acts individually or jointly in processing Personal Data on behalf of the Personal Data Controller. So, it can be understood that the personal data processor is the party that performs the processing at the direction of the controller. In this case, company X, which is tasked with processing data on workers' working hours and making wage payments to these workers, is a personal data processor because it acts on behalf of the personal data controller to carry out data processing in accordance with the purposes of the personal data controller.

Between these parties, there are 3 types of agreements that can be produced, namely: **Between the Controller and the Personal Data Controller**. In connection with the illustration above, the agreement between the developer and the outsourcing company is an agreement between the two personal data controllers to determine the purpose of using the personal data to the personal data processor. Arrangements for the agreement between controllers and personal data controllers themselves can be found in Article 18 of the PDP Law: Processing of Personal Data can be carried out by 2 (two) or more Personal Data Controllers. If Personal Data Processing is carried out by 2 (two) or more Personal Data Controllers, it must meet the minimum requirements: There is an agreement between the Personal Data Controllers which contains roles, responsibilities, and relationships between Personal Data Controllers; There are purposes that are interrelated with the method of processing Personal Data that are determined jointly; and There is a contact person appointed jointly". **Between the Controller and the Personal Data Processor**. This is implicitly seen in the meaning of personal data processors who process Personal Data on behalf of personal data controllers (vide. Article 1 number 5 PDP Law). In connection with the illustration above, the agreement between the developer and the outsourcing company with company X is an agreement between the controller and processor of personal data, namely the developer and outsourcing company as the controller, and company X as the processor of personal data. This agreement is made possible by Article 51 PDP Law: "In the event that the Personal Data Controller appoints a Personal Data Processor, the Personal Data Processor is obliged to process Personal Data based on the order of the Personal Data Controller". **Between the Processor and the Personal Data Processor**. In connection with the illustration above, if in practice company X cooperates with other companies to participate in personal data processing

activities, then based on Article 51 paragraph (4) PDP Law, personal data processors can involve other personal data processors in processing personal data. So that the agreement formed between Company X and the other company that is partnered with is an agreement between the processor and the processor of personal data. However, this agreement must obtain written approval from the personal data controller (vide. Article 51 paragraph (5) of the PDP Law).

Thus, similar to the provisions in the ITE Law, the PDP Law does not have rigid provisions regarding agreements that can result from a legal relationship between the two parties. But what distinguishes it from the ITE Law is that the PDP Law only recognizes personal data controllers and processors, in contrast to the ITE Law which recognizes three parties, namely ESO, Electronic System Users, and Electronic Agents. However, this difference in terminology is common because the ITE Law and its implementing regulations do not only discuss the protection of personal data in a *lex specialis* manner, so they do not specifically refer to personal data processing activities. Whereas in the PDP Law, ESO can play a role as either a controller of personal data or a processor of personal data, depending on the status and activity of processing personal data as a controller or simply processing the personal data.

Personal Data Processing Agreement Under European Union Law

GDPR distinguishes two types of parties in data processing, namely controllers and processors (Treacy, 2017). Based on Article 4 paragraph (7) GDPR, the controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...". In other words, the controller is the party that determines the reasons and purposes for processing personal data. Meanwhile, based on Article 4 paragraph (8) GDPR, the processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". In other words, the processor must be separate from the controller. If related to the illustration, the developer and the outsourcing company are controllers because together they determine the purpose of data processing, namely processing personal data to determine workers' rights as well as paying wages to workers. Meanwhile, company X and the check-clock application are processors, namely the party that processes workers' personal data according to the instructions of the developer and the outsourcing company.

Based on the two types of parties in the processing of personal data, the GDPR regulates three types of data processing agreements, namely joint-control agreements, controller-processor agreements, and processor-processor agreements:

Between the Processor and the Personal Data Processor. In accordance with article 4 paragraph (7) GDPR, controllers can individually or jointly determine the purposes and means of data processing. If two controllers jointly determine ends and means data processing, the two are called joint-controllers and must agree on a joint-control agreement (Colcelli, 2019), as stipulated in Article 26 paragraph (1) GDPR: Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by the Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects. The GDPR does not regulate in detail the contents of the joint-control agreement, but what is clear is that the agreement must reflect the roles, obligations and responsibilities of each controller (Colcelli, 2019). The joint-control agreement must be accessible to the data owner (vide. Article 26 paragraph (2) GDPR)

Controller-processor agreement. As regulated in Article 4 paragraph (8) GDPR, the controller can ask the processor to process the data it has. In this case, Article 28 paragraph (3) GDPR requires the controller and processor to have an agreement that regulates "the subject matter and duration of processing, the nature and purpose of processing, the type of personal data and the category of data subject, as well as the obligations and rights of the controller Van (Van Alsenoy, 2016). Even the agreement must include the processor's obligations in detail, including: process personal data only on the basis of instructions from the controller, including with respect to the transfer of personal data to a third country or international organization, unless required to do so by the laws of the Union or Member State that is the subject of processing; in such cases, the processor must inform the controller of the legal requirements before processing, unless the law prohibits the information on important public interest grounds; ensure that the person authorized to process personal data has committed to confidentiality or is under appropriate

confidentiality obligations; take all measures to ensure the security of the processing of personal data; may involve other processors; considering the nature of the processing, assist the controller with appropriate technical and organizational measures, to the extent possible, for the fulfillment of the controller's obligations to respond to requests to exercise assigned data subject rights; assist the controller in ensuring compliance with compliance obligations taking into account the nature of the processing and the information available to the processor; at the controller's option, delete or return all personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless statutory law requires the retention of personal data; and provide the controller with all information necessary to demonstrate compliance with the obligations set out in this Article and allow for and contribute to audits, including inspections, conducted by the controller or other auditors mandated by the controller.

Processors agreement. GDPR also allows inter-processors to work together to process data, the party that works together with the main processor is called a sub-processor. The processors must have separate written agreements (Cruz, 2020), as stated in Article 28 paragraph (2) GDPR. Furthermore, based on Article 28 paragraph (4) GDPR, the matters agreed upon in the controller-processor agreement also apply to sub-processors that work together with the main processor: "Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation". From the description above, the GDPR distinguishes between two types of parties processing personal data based on their roles, namely controllers and processors; the controller plays the role of determining the reasons and purposes for processing personal data; The processor plays the role of processing personal data on behalf of the controller. Apart from that, the GDPR also differentiates agreements personal data processing into three, namely joint-control agreement, controller-processor agreement, and processor-processor agreement.

After analyzing the relevant legal regulations, it can be understood that the personal data processing agreements in Indonesia and the European Union have some similarities and differences. The similarity is that both laws in these countries allow two or more parties to process personal data together, of course, provided that each party is committed to applying the principles of personal data protection. While the difference lies in the parties and the type of agreement regulated in the laws and regulations of each country. The similarities and differences regarding the personal data processing agreement in Indonesia and the European Union will be described in the table below:

Table 1. Comparison of Personal Data Processing Agreements in Indonesia and the European Union

Indicator	Indonesia	European Union
Similarities: allow two or more parties to process personal data jointly		
Parties	1. Controller (ESO, Electronic System User) 2. Processor	1. Controller 2. Processor
Types of Agreement	1. Between the Controller and the Personal Data Controller 2. Between the Controller and the Personal Data Processor 3. Between the Processor and the Personal Data Processor Personal Data Processing Agreement (freedom of contract); the government does not actively intervene to determine the contents of the agreement	1. Joint-control agreement 2. Controller-processor agreement 3. Processor-processor agreement The government intervened to determine the contents of the agreement

Liability for Data Protection: Indonesia vs European Union

Liability is the obligation of legal subjects to pay compensation to owners of personal data for their actions. The action in question is if there is a failure in the protection of personal data, for example there is a leak of personal data, a hacker attack, etc (Situmeang, 2021). In order to simplify the discussion, the term used in this sub-chapter is ESO, but Electronic System Users, Electronic Agents, controllers and processors are also included. This sub-discussion will analyze who is the party responsible for the failure of personal data protection if the processing of personal data is carried out by more than one ESO or personal data processors together and how the mechanism for obtaining compensation is. To facilitate understanding, an illustration will be made: For example, in processing worker data, it turns out that a hacker attack occurs, so that the personal data of workers is stolen by hackers. Knowing this, workers, as owners of personal data feel aggrieved and want to sue for compensation.

The Responsibility of Electronic System Operators in Failure to Protect Personal Data According to Indonesian laws

As described above, if data processing is carried out by more than one party, the legal relationship between them is regulated in a personal data processing agreement. Personal data processing agreements in Indonesia are still dominated by the principle of freedom of contract, in other words, the government's intervention as a public authority is very minimal, including regarding accountability in the event of a failure to protect personal data. One of the arrangements regarding ESO liability is in Article 21 ITE Law: 1) Senders or Recipients may carry out Electronic Transactions themselves, through parties authorized by them, or through Electronic Agents; 2) Parties who are responsible for all legal consequences in the implementation of Electronic Transactions as referred to in paragraph (1) are regulated as follows if done alone, all legal consequences in the implementation of Electronic Transactions shall be the responsibility of the transacting parties; if it is done through the granting of a power of attorney, all legal consequences in the implementation of Electronic Transactions shall be the responsibility of the authorizing agent; or if carried out through an Electronic Agent, all legal consequences in the implementation of Electronic Transactions shall be the responsibility of the Electronic Agent operator; 3) If the loss of an Electronic Transaction is caused by the failure of the Electronic Agent to operate

because of a third party's action directly against the Electronic System, all legal consequences shall be the responsibility of the Electronic Agent operator; 4) If the loss of an Electronic Transaction is caused by the failure of the Electronic Agent to operate due to the negligence of the service user, all legal consequences are the responsibility of the service user; 5) The provisions referred to in paragraph (2) do not apply in the event that force majeure, errors and/or negligence of the Electronic System user can be proven.

The article above regulates the liability of Electronic Agents, where Electronic Agents are obliged to pay compensation in the event of a failure in protecting personal data, unless it can be proven that the failure was due to user error or due to force majeure (Wijaya & Purwanto, 2019). If related to the illustration, the Electronic Agent, in this case the check-clock application, will be held liable if it is proven that the system was hacked by hackers. In addition to the liability of the Electronic Agent described above, other ESO responsibilities depend on the agreement of the parties, whether the responsibility is delegated to one party or jointly responsible. Of course, this is risky, especially if the ESOs have a subordinate position, then the stronger party will tend to shift the blame onto the weaker party. If it is linked in the illustration, then in this case there is no prohibition for developers and outsourcing companies to delegate all liability to company X as ESO. The systematics of liability in the PDP Law is slightly different from the ITE Law. Implicit arrangements regarding the relationship between controller and personal data processor accountability are regulated in Article 51 of the PDP Law mentioned "If the Personal Data Controller appoints a Personal Data Processor, the Personal Data Processor is obligated to process Personal Data based on the order of the Personal Data Controller; The processing of Personal Data as referred to in paragraph (1) is carried out in accordance with the provisions stipulated in this Law; and Processing of Personal Data as referred to in paragraph (1) is included in the responsibility of the Personal Data Controller".

Thus, it can be understood that in the event of a personal data protection failure, even if it is done by a personal data processor, responsibility and accountability will still be borne by the personal data controller. This becomes part of the obligations of personal data controllers in Article 47 PDP Law, namely: "Personal Data Controllers must be responsible for the processing of Personal Data and show accountability in the obligation to implement the principles of Personal Data Protection." However, it also does not rule out the possibility for the owner or subject of

personal data to be harmed by the failure of personal data protection to sue the personal data processor. This is because the obligations of the personal data controller also apply to personal data processors (*vide*. Article 52 PDP Law). So that the owner or subject of personal data can sue the personal data processor for negligence in maintaining the obligations contained in the laws and regulations. As for practice, the subject or owner of personal data often does not know that the personal data controller enters into an agreement with the personal data processor to carry out further personal data processing, so that if this happens, the PDP Law still allows accountability to still be borne by the personal data controller.

Regarding the compensation mechanism in the event of a personal data protection failure, it is the owner or subject of the personal data who is harmed. The owner or data subject has the right to sue and receive compensation for violations of processing personal data about himself in accordance with statutory provisions (vide. Article 12 PDP Law). The owner or subject of personal data can also file a complaint with Minister as an effort to resolve disputes by deliberation or other alternative dispute resolution (vide. Article 29 PERMENKOMINFO PDP jo. Article 64 paragraph (1) PDP Law). If they do not get a settlement, the owner of the personal data can file a civil lawsuit (vide. Article 32 paragraph (2) PERMENKOMINFO PDP).

As regulated in Article 14 paragraph (3) PP PSTE jo. Article 20 paragraph (2) of the PDP Law, the processing of personal data is mandatory with the consent of the owner of the personal data. In other words, there is an agreement between the personal data owner and ESO as the controller or processor of personal data. Thus, in this civil lawsuit, the owner of personal data can sue all ESO or only one of the ESO based on default. If compensation payments are made by certain ESOs, then these ESOs can sue other ESOs who process personal data with them, to replace the compensation they have paid, provided that the ESOs agree to be jointly liable. This scheme is a liability in a joint liability or joint liability agreement as stipulated in Articles 1278 to Article 1295 BW, where payments made by one debtor free the other debtor, without reducing the rights of the debtor who pays to sue the other debtor (Bakarbessy & Anand 2018). For example, if the worker only sues the outsourcing company, then it is the outsourcing company that must pay compensation, then after that the new outsourcing company can sue the developer, electronics agent and/or company X as a ESO to reimburse the compensation money or compensation that has been paid.

Because the legal relationship of the ESOs is regulated in the data processing agreement, the outsourcing company can sue other ESOs on the basis of a default claim to replace the compensation that has been paid. Based on Article 1267 BW, the things that can be prosecuted include (Hernoko, 2014). Contract fulfillment and Compensation. Based on Article 1243 BW, compensation includes costs (*kosten*), losses (*schaden*), and interest (*interssen*). Costs are actual expenses e.g. attorneys' fees, damages paid by ESO to owners of personal data. Loss is the declining value of an object. While interest is the profit expected by creditors (Bakarbessy & Anand 2018): Contract termination, Fulfillment of contracts and compensation, and Termination of the contract along with compensation.

BW lays down limitations in determining compensation to be paid by parties who violate the agreement, namely in Article 1247 BW, Article 1248 BW, and Article 1250 BW, including (Bakarbessy & Anand 2018): Foreseeable losses when entering into contracts and Loss as a direct result of default. The theory of causality that is commonly used is the adequate theory where the loss experienced is a direct and instant result of default. Interest determined by law is called moratory interest, which is 6% per year unless otherwise determined by the parties (vide. Stb.1848-22 jo. Stb. 1849-63).

From the description above, the ITE Law and its implementing regulations only regulate the liability of Electronic Agents, while the liability of ESO and Electronic System Users is regulated based on an agreement. Meanwhile, the PDP Law regulates intermediary liability between Personal Data Processors and Controllers. In the failure of personal data protection, ESO as the controller or processor of certain personal data that pays compensation to the owner of the data can sue another ESO based on default to replace the compensation that has been paid, as long as it is agreed that the ESO is jointly responsible.

Liability of Electronic System Operators in Failure to Protect Personal Data According Compared to The European Union

In contrast to Indonesia, the intervention of the European Union government in determining which ESO is responsible in the event of a personal data protection failure is quite large. The description of the articles that regulate this matter include:

Article 82 mentioned 1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered; 2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with the obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller; 3) A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage; 4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraph 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject; 5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the corresponding compensation to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2; and 6) Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79 paragraph (2).

Article 28 paragraph (4) mentioned where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processors by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Article 28 paragraph (10) mentioned If a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing. The important points gleaned from the descriptions of the above

articles include: In the event of a personal data protection failure, each controller and processor must be held accountable (vide. Article 82 paragraph (4) GDPR); In a joint-controller, although each is responsible, it does not mean that the controllers have equal accountability (Colcelli, 2019); The new processor is liable if it does not fulfill the obligations regulated in the GDPR and/or acts outside the controller's instructions (vide. Article 82 paragraph (2) GDPR); If the processor determines the purpose and means of processing personal data, then the processor is considered a controller (vide. Article 28 paragraph (10) GDPR); and if the processor appoints a sub-processor to process personal data, then the main processor is the party responsible in the event of a personal data protection failure, even though the sub-processor is the one who made the mistake (vide. Article 28 paragraph (4) GDPR). If related to the illustration, then the developer and outsourcing company as the controller are the responsible parties, while company X and the check-clock application as a new processor are also responsible if it is proven that the hacker attack was caused by poor system security.

Regarding the mechanism for obtaining compensation, based on Article 82 paragraph (6) GDPR, compensation or compensation must be demanded by the owner of personal data through the courts. The data owner can sue each controller (Nemčeková, 2019), as stipulated in Article 26 paragraph (3) GDPR: "Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers". If only one controller or processor pays all compensation, then the controller or processor can claim compensation from the other controller and or processor (vide. Article 82 paragraph (5) GDPR) (Colcelli, 2019). Because the legal relationship between ESOs is based on an agreement, compensation is demanded based on default (breach of contract). So in terms of workers who sue the outsourcing company, then after paying compensation, the outsourcing company can demand reimbursement of compensation money from the developer, and company X as well as the check-clock application (if proven to have violated the obligations under the GDPR).

Comparative Analysis of the Liability of Electronic System Operators in the Failure of Personal Data Protection in Indonesia and the European Union

From the description above, it can be seen that there are more differences than similarities regarding ESO liability in the failure of personal data protection in Indonesia and the European

Union. The only similarity is in the mechanism for obtaining compensation, where if only certain ESO pays all compensation, then the ESO can claim compensation from other ESO who are also liable based on default. Meanwhile, the main striking difference is in terms of determining which ESO is liable; in Indonesia in the ITE Law this is determined by the agreement of the parties in the data processing agreement, except for the responsibility of Electronic Agents which has been regulated separately, whereas in the PDP Law it has similarities with the EU GDPR, namely the controller of personal data is the party who is responsible unless the personal data processor violates obligations under the law or acting outside the order of the personal data controller; in the European Union the responsible party has been determined by the GDPR, where basically the controller is responsible for the failure of personal data protection, while the new processor is liable if it is proven that the processor has violated the obligations set by the GDPR and/or acted outside the controller's instructions. Especially if the processor cooperates with a sub-processor, the main processor is responsible for the fault of the sub-processor it designates. Comparison of ESO liability in personal data protection failure can be seen in the table below:

Table 2. Comparison of Liability of Electronic System Operators in Personal Data Protection Failures in Indonesia and the European Union

Indicator	Indonesia	European Union
Similarities: a compensation mechanism, where ESO or in the PDP Law is the controller of personal data who pays all compensation can sue other ESO who are also liable based on default		
Liable parties	1. ITE Law: Determined by the parties based on the agreement in the data processing agreement. 2. PDP Law: Personal Data Controller The Personal Data Processor, in breach of its obligations, acts contrary to the orders	1. *Controller* 2. *Processor*, only, if it violates its obligations, acts outside the controller's instructions, and/or the sub-processor it appoints makes an error in processing personal data

	and objectives of the personal data controller, and other data processors commit errors

CONCLUSION

Indonesian and EU regulation are both allow two or more parties to process personal data together, while the difference lies in the parties and the type of agreement stipulated in the laws and regulations of each country. The ITE Law in Indonesian law recognizes several parties that process personal data, namely ESO, Electronic System Users and Electronic Agents, where the legal relationship is regulated in a data processing agreement. Meanwhile, the PDP Law recognizes personal data controllers and personal data processors. European Union law also recognizes two types of personal data processing parties, namely controllers and processors, and three types of personal data processing agreements, namely joint-control agreements, controller-processor agreements, and processor-processor agreements. The similarities of ESO's liability in terms of failure to protect personal data according to Indonesian and European Union law is the mechanism for claiming compensation, to wit the who paid all compensation to the owner of the data has the right to claim compensation from other ESOs who are also liable based on default. Regarding the difference, there is a determination of the responsible party, where based on Indonesian law, in the ITE Law the party responsible is determined by the parties themselves based on an agreement, except for the responsibility of Electronic Agents which has been specified in the ITE Law, and in the PDP Law ESO as controller personal data is liable unless the personal data processor is found to have violated statutory obligations and acted outside the order of the personal data controller. Not much different from the PDP Law, in the European Union it has determined that the controller must be held accountable, while the new processor is liable if it violates its obligations regulated by the GDPR, acts outside the controller's instructions, and/or the processor appointed by it makes an error in processing personal data.

ACKNOWLEDGMENTS

None.

REFERENCES

Anand, G. (2011). Prinsip Kebebasan Berkontrak dalam penyusunan kontrak. *Yuridika*, 26(2), 91-101.

Baiq, P. A. (2021). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif. *DIKTUM: Jurnal Syariah dan Hukum*, *19*(2), 149-165.

Bakarbessy, L., & Anand, G. (2018). *Buku Ajar Hukum Perikatan.* Sidoarjo: Zifatama Jawara.

Brkan, M. (2019). The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning. *German Law Journal*, *20*(6), 864-883.

Colcelli, V. (2019). Joint Controller Agreement Under Gdpr. *EU and comparative law issues and challenges series (ECLIC)*, 3, 1030-1047.

Cruz, R, D, L. (2020). Data Protection Contracts — What Tends To Be Missing and What To Do About It. *Pivacy and Data Protection*, 20(8), 2-17.

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, *5*(2), 177-199.

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289-304.

GDPR Register. (2022). *"Data Processing Agreement (DPA)*, online: GDPR Register ‹https://www.gdprregister.eu/gdpr/data-processing-agreement-dpa/›.

Hernoko, A, Y. (2014). *Hukum Perjanjian: Asas Proporsionalitas Dalam Kontrak Komersial.* Jakarta: Prenadamedia Group.

Kadly, E. I., Rosadi, S. D., & Gultom, E. (2021). Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. *Jurnal Sains Sosio Humaniora*, 5(1), 199-212.

Kurniawan, F., Nugraha, X., Abrianto, B. O., & Ramadhanti, S. (2020). The Right To Access Banking Data In a Claim For A Divisio Of Combined Assets That Is Filed Separately From A Divorce Claim. *Yustisia Jurnal Hukum*, *9*(1), 37-45.

Muhammad, M. O., & Nugroho, L. D. (2021). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce yang Terdampak Kebocoran Data Pribadi. *Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo*, *14*(2), 165-174.

Nemčeková, I. (2019), *Liability of Joint Controllers in the Light of the CJEU Case Law*, online: INPLP https://inplp.com/latest-news/article/liability-of-joint-controllers-in-the-light-of-the-cjeu-case-law/

Nursiyono, J. A., & Huda, Q. (2023). Analisis Sentimen Twitter Terhadap Perlindungan Data Pribadi Dengan Pendekatan Machine Learning. *Jurnal Pertahanan & Bela Negara*, *13*(1), 1-16.

Putra, C. A. G., Budiartha, I. N. P., & Ujianti, N. M. P. (2023). Perlindungan Hukum Terhadap Konsumen dalam Persfektif Kesadaran Hukum Masyarakat. *Jurnal Konstruksi Hukum*, *4*(1), 13-19.

Saputra, R. D., Rachim, K. V., & Taniady, V. (2023). Empowering Voices: Building an Electronic Petition System for Strengthening Freedom of Speech in Indonesia. *Journal of Judicial Review*, *25*(1), 71-88.

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Sasi*, *27*(1), 38-52.

Tektona, R. I. (2023). Kepastian Hukum Pemilik Data Pribadi Dalam Aplikasi Satu Sehat. *Jurnal Legislasi Indonesia*, *20*(1), 28-41.

Treacy, B. (2017). Working Party Confirms 'controller 'and 'processor 'distinction. *Privacy and Data Protection*, 8(8), 3-5.

Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53-84.

Van Alsenoy, B. (2016). Liability under EU data protection law: from Directive 95/46 to the General Data Protection Regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *7*, 271.

Wijaya, I. P. A. D., & Purwanto, I. W. N. (2019). Perlindungan Hukum Dan Tanggung Jawab Para Pihak Dalam Transaksi Bisnis Elektronik Di Indonesia. *Kertha Negara*, *7*(10), 1-16.