**International Journal of Applied Review**
**www.multiappliedjournal.com**
**E-ISSN: 3107-8443**
**Received: 29-06-2026, Accepted: 29-07-2026, Published: 13-08-2026**
**Volume 2, Issue 3, 2026, Page No. 5-9**

# Legal compliance in data processing agreements between personal data controllers and personal data processors in Indonesia's retail sector

**Trevira Aulia Belqies Marpaung*, Diah Aju Wisnuwardhani, Fitria Dewi Navisa**
Faculty of Law, Universitas Merdeka Malang, Indonesia
**Corresponding Author:** Trevira Aulia Belqies Marpaung
**DOI:** https://doi.org/10.66856/ijsps.2026.2.3.2105

**Abstract**
The development of retail business activities in the digital world has caused the processing of customers' personal data to be carried out not only by retail companies, but also by various service providers, such as cashier systems, payment services, applications, data storage, digital marketing, customer service, and delivery services. The involvement of multiple parties creates the need to clarify the legal relation between the Personal Data Controller and the Personal Data Processor through a Data Processing Agreement. Thus, the article aims to analyze the adequency of the obligations and responsibilities of Personal Data Controllers and Personal Data Processors under Law Number 27 of 2022 on Personal Data Protection to ensure a legal compliance system in the retail sector. The article employs a normative legal research method with a statutory, conceptual, comparative, and limited case approaches. Results show that the regulation of the obligations and responsibilities of Personal Data Controllers and Personal Data Processors is not yet fully adequate at the level of contractual relation and implementation mechanisms. Several gaps remain in relation to things such as documented instructions, due diligence of Processors, minimum clause standards, Processor assistance, audits and evidence of compliance, early notification of Personal Data Protection failures, the use of other Personal Data Processors, and the deletion or return of Personal Data after the processing relation ends. Therefore, we argue that there is a need for the formulation of a layered normative model of a legal compliance system, consisting of compliance principles, internal and external compliance parameters, minimum clause standards, and mechanisms for implementation and accountability.

**Keywords:** Personal data controller, personal data processor, data processing agreement

## Introduction

Digitalization of the retail business has changed the pattern of relationships between companies and customers. Transactions are no longer done physically, but can also be done through electronic commerce, applications, loyalty programs, digital payment systems, customer service, digital marketing, and other delivery services. By participating in the transaction of the digital world, each of these channels may involve the processing of customers' Personal Data, such as names, addresses, phone numbers, e-mail addresses, transaction histories, purchasing preferences, and delivery locations. [1]

In practice, Personal Data Processing in the retail sector is rarely carried out entirely by the retail company itself. Companies may involve several providers outside of the company itself, such as cashier system providers, payment service providers, cloud-based storage providers, application providers, customer service providers, digital marketing providers, and delivery companies. The involvement of these parties raises legal questions relating to their position, since not all parties that access or process data have the same legal position. A party may be a Personal Data Controller if it determines the purposes of and exercises control over the processing, while another party may be a Personal Data Processor if it processes data on behalf of the controller. [2]

Law Number 27 of 2022 on Personal Data Protection has provided a normative basis for the relationship between Personal Data Controllers and Personal Data Processors. Furthermore, Article 1 points (4) and (5) distinguish the legal positions of the two parties. Article 51 provides that the processor carries out processing based on the order of the controller, while Article 52 extends several controller obligations to the processor according to the scope of processing performed. These provisions show that Indonesian law recognizes a division of roles between controllers and processors.

Nevertheless, this regulation has not fully answered the need for contractual relationships in practice. The Personal Data Protection Law does not expressly determine that the appointment of a processor must be set out in a Data Processing Agreement. The law also does not determine the form of the agreement, its position in relation to the main service agreement, or the minimum clauses that must be included. As a result, the implementation of Personal Data Protection obligations in business relationships is often placed only in confidentiality clauses or general provisions on information security. [3]

Confidentiality clauses are important, but they are not always sufficient to regulate all aspects of processing. The relationship between a Controller and a Processor requires provisions on the purpose and duration of processing, types of Personal Data, categories of Personal Data Subjects, Controller instructions, Processor assistance, audits, handling of Personal Data Protection failures, the use of other Personal Data Processors, deletion or return of data, and allocation of responsibility. [4] Without such provisions in detail, the legal obligations established by the law that only governs the general principle are risky since those agreements are most likely unable to be implemented, supervised, and proven adequately.

As comparative material, Article 28 of the General Data Protection Regulation (GDPR) by the European Union (EU) provides more detailed regulation concerning the relationship between Controllers and Processors. The article has made a specific requirement for a contract or other binding legal instrument, containing documented instructions, confidentiality, security, assistance to the Controller, use of other Processors, audits, and deletion or return of Personal Data after the processing ends. Although the GDPR is not applicable as a prevailing regulation in Indonesia, the principles in Article 28 can be used as comparative material to identify aspects that have not been regulated in detail under national law.

Previous studies have discussed various aspects of Personal Data Protection, such as the roles of Controllers and Processors, notification of Personal Data Protection failures, consent, risk management, and liability for data misuse. However, these studies have not specifically formulated a normative model of a legal compliance system in Data Processing Agreements in the retail sector. Therefore, this article focuses on the legal issue concerning the obligations and responsibilities of Personal Data Controllers and Personal Data Processors under Law Number 27 of 2022 to ensure a legal compliance system in the retail sector. This article is written to support the idea that there is a need to have a specific normative model of a legal compliance system in Data Processing Agreements to ensure legal certainty, accountability, and Personal Data Protection.

## Research Method

This article employs a normative legal research method because the nature of the study lies in norms, principles, concepts, and legal doctrines governing the relationship between Personal Data Controllers and Personal Data Processors. The approaches used are statutory, conceptual, and comparative approaches. The statutory approach is used to examine Law Number 27 of 2022 on Personal Data Protection, the Indonesian Civil Code, and other prevailing regulations relating to the implementation of electronic systems. The conceptual approach is used to discuss the concepts of Personal Data Controller, Personal Data Processor, Data Processing Agreement, legal compliance system, legal responsibility, and legal protection. The comparative approach is used by placing Article 28 of GDPR as comparative material, not as law directly applicable in Indonesia.

This article is analyzed by using legal materials consisting of primary legal materials and secondary legal materials. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, the Indonesian Civil Code, Law Number 27 of 2022 on Personal Data Protection, the Electronic Information and Transactions Law and its amendments, Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions, as well as the EU's General Data Protection Regulation (GDPR) as a comparative material. The legal materials are analyzed normatively and prescriptively by assessing the adequacy of national regulation, comparing it with relevant principles, and formulating a normative model of a legal compliance system.

## Results and Discussion

### 1. Legal Relation between Personal Data Controllers and Personal Data Processors in the Retail Sector in Indonesia

The legal relation between Personal Data Controllers and Personal Data Processors in the retail sector has characteristics that differ from ordinary service relations. In the retail sector, customer data may be processed since the first stage of account creation up until other stages like transactions, payments, delivery of goods, customer service, promotions, and loyalty programs. Such data is not only stored in the internal systems of retail companies, but may also be stored in systems that belong to other parties that provide supporting services. [5]

This condition requires the legal position of the parties to be determined functionally. Cashier system providers, payment service providers, application providers, data storage providers, digital marketing providers, customer service providers, and delivery service providers may access Personal Data, but their legal positions are not always the same. A party may act as a Processor if it only processes data on behalf of and based on the instructions of the retail company. However, that party may become a Controller if it determines the purposes of processing by itself or uses Personal Data for its own interests.

In this context, the designation of parties in a contract is not always sufficient. Terms such as service provider, partner, vendor, or third party do not determine whether the party is a Controller or a Processor. The determination must be based on who determines the purpose of processing, who controls the main means of processing, who gives instructions, and who uses the Personal Data. This approach is important because the allocation of obligations and responsibilities under the Personal Data Protection Law is based on the functions performed, not merely on the name of the position written in the agreement.

In Indonesia, Law Number 27 of 2022 concerning Personal Data Protection has provided a basis for distinguishing these two positions. A Personal Data Controller is a party that determines the purposes and exercises control over the Processing of Personal Data, while a Personal Data Processor is a party that processes data on behalf of the Controller. Article 51 then affirms that the Processor must act based on the order of the Controller. If the Processor processes data outside the order and purpose of the Controller, responsibility for such processing lies with the Processor. [6]

This regulation provides an important foundation for the relationship between Controllers and Processors. However, in the practice of the retail sector, this foundation still requires operational regulation. Controllers need information from Processors to fulfill the rights of Personal Data Subjects, conduct supervision, assess risks, and handle Personal Data Protection failures. If assistance, reporting, audit, and evidence of compliance obligations are not clearly regulated, the legal relationship between Controller and Processor risks stopping at a general division of roles, without an adequate implementation mechanism.

### 2. Adequacy of the Prevailing Regulation in Ensuring a Legal Compliance System

The regulation of the obligations and responsibilities of Personal Data Controllers and Personal Data Processors under Law Number 27 of 2022 can be assessed as adequate

at the level of basic norms. This is reflected in the distinction between the positions of Controllers and Processors, the obligation of Processors to act based on the order of Controllers, the extension of certain obligations to Processors, written approval for the use of other Personal Data Processors, and the responsibility of Processors when acting outside the order and purpose determined by the Controller.

However, the regulation is not yet fully adequate to ensure a legal compliance system at the level of contractual relationships, which may impact its implementation. A legal compliance system cannot be supported only by the existence of general norms. It requires clear obligations, allocation of functions, implementation procedures, supervision mechanisms, evidence of compliance, and legal consequences when obligations are not fulfilled. In the relationship between Controller and Processor, these elements should be set out in a Data Processing Agreement. This issue creates several gaps in the personal data protection law.

The first gap lies in processing instructions. The Personal Data Protection Law has determined that the Processor acts based on the order of the Controller, but it has not regulated the form of such an order. There is no provision on whether instructions must be written, who is authorized to give instructions, how instructions are changed, or how instructions are proven in the event of a dispute. In fact, instructions are the main basis for assessing whether a Processor acts within its authority or has processed data outside the Controller's order. [7]

The second gap relates to due diligence before appointing a Processor. In retail activities, the selection of service providers is often based on business needs, price, and technical capability. However, from the perspective of Personal Data Protection, the Controller should also assess the Processor's ability to maintain security, manage data, provide information, and demonstrate a compliance record. As a comparison, Article 28, paragraph (1) of GDPR stipulates that a Controller may only use Processors that provide sufficient guarantees to implement appropriate technical and organizational measures. This principle is relevant to be adapted because the selection of Processors is part of the Controller's responsibility. [8]

The third gap concerns the minimum clause standards of Data Processing Agreements. The Personal Data Protection Law has not regulated in detail the elements that must be included in the contractual relationship between Controllers and Processors. As a result, agreements that only contain confidentiality clauses may be considered sufficient in practice, even though they do not regulate the scope of processing, types of data, categories of Personal Data Subjects, Processor assistance, audits, incident reporting, use of other Processors, and termination of processing. These aspects are necessary so that legal obligations can be implemented and proven.

Another gap concerns Processor assistance, audits, and evidence of compliance. In many retail activities, customer data is stored in systems managed by Processors. Therefore, Controllers need assistance from Processors to follow up on requests for access, correction, deletion, objection, or other rights of Personal Data Subjects. Controllers also need information to assess whether Processors have fulfilled security and confidentiality obligations. Without the right to obtain information or conduct proportionate audits, the Controller's supervision obligation is difficult to implement effectively. The use of other Personal Data Processors is also not adequately regulated. The Personal Data Protection Law indeed requires written approval from the Controller before the Processor involves another Processor. However, there is no further regulation on the form of approval, the information that must be provided, the Controller's right to object, the flow-down of obligations to other Processors, and the responsibility of the main Processor. In digital practice, application providers or data storage service providers may involve other parties in the processing chain. [9]

From these analyses, it can be seen that the Personal Data Protection law in Indonesia still shows the inadequency of the importance of coordination between Controllers and Processors. The Personal Data Protection Law has regulated notification obligations in the event of Personal Data Protection failures. However, in terms of legal relationships involving Processors, initial information concerning incidents is often held by Processors themselves. Therefore, there needs to be regulation on the Processor's obligation to immediately notify the Controller of the incident, including initial information, timelines, temporary measures, and handling documentation. Overall, the regulation relating to the legal relation between Processor and Controller in Indonesia can be said as partially adequate. The regulation is adequate at the level of basic norms, but not yet fully adequate at the level of contractual relationships and implementation mechanisms. The existence of these gaps does not mean that Data Processing Agreements cannot be made under Indonesian law. On the contrary, based on the principle of freedom of contract under the Indonesian Civil Code, the parties may form Data Processing Agreements as innominate contracts. However, to ensure that such agreements can support a legal compliance system, a normative model is needed that contains principles, parameters, minimum clauses, and accountability mechanisms.

## 3. Normative Model of a Legal Compliance System in Data Processing Agreements

Since there are some gaps in the Personal Data Protection law, there needs to be a certain model to fill the gaps so that the regulation can be implemented in a better way. The normative model of a legal compliance system in Data Processing Agreements is formulated to bridge the general norms under the Personal Data Protection Law with the need to implement obligations in retail business relationships. This model is not intended to replace the law, but to translate legal obligations into a contractual structure that is more operational, supervisable, and provable.

The proposed model is a layered model. The first layer is the principle of compliance. This principle emphasizes that the relationship between Controller and Processor must be identifiable, directed, supervised, and accountable. This means that the parties need to determine their respective legal positions, limit the purposes of processing, document instructions, apply risk-based security, provide assistance, allow supervision, and have recovery mechanisms in the event of Personal Data Protection failures. [10]

The second layer is internal and external compliance parameters. Internal compliance relates to the governance of the relationship between Controller and Processor, such as determining the positions of the parties, mapping processing activities, conducting due diligence, providing instructions, limiting access, keeping records, conducting audits, and

implementing corrective actions. External compliance relates to obligations toward Personal Data Subjects and competent authorities, such as the fulfillment of Personal Data Subject rights, notification of Personal Data Protection failures, provision of information, and responsibility for losses.

The third layer is the minimum clause standards. A Data Processing Agreement should at least contain the identity and legal position of the parties, subject matter and duration of processing, nature and purpose of processing, types of Personal Data, categories of Personal Data Subjects, Controller instructions, confidentiality and security obligations, Processor assistance, audits, use of other Personal Data Processors, handling of Personal Data Protection failures, deletion or return of data, allocation of responsibility, and dispute settlement. These clauses are not intended as rigid standard forms, but as minimum limits so that the agreement does not become merely an ordinary service agreement.

The fourth layer is the mechanism for implementation and accountability. This mechanism includes due diligence before appointing a Processor, risk assessment, documented instructions, monitoring, audits, incident escalation, corrective actions, control over other Processors, termination of processing, and dispute settlement. These mechanisms are required so that legal obligations do not remain general statements, but can be implemented through concrete actions. [11]

Due diligence needs to be placed as an initial stage before the Controller appoints a Processor. In the retail sector, the depth of due diligence may be adjusted to the type of service and processing risk. Delivery service providers may require a different assessment from payment system providers, customer application providers, or cloud-based storage providers. However, the basic principle remains the same, namely that the Controller needs to ensure that the Processor has adequate capability to process data securely and responsibly.

Audit also needs to be understood proportionately. An audit does not always have to be a direct examination of all Processor systems. It may be conducted through compliance reports, certifications, technical evidence, activity records, or periodic examinations according to the level of risk. The important point is that there must be a basis for the Controller to assess and prove that the Processor has fulfilled the agreed obligations.

The use of other Personal Data Processors must be controlled through Controller approval, notification of changes, flow-down of obligations, and responsibility of the main Processor. If the main Processor involves another party, equivalent Personal Data Protection obligations must be passed on to that party. The main Processor also remains responsible to the Controller for the performance of obligations by the other Processor it involves. The handling of Personal Data Protection failures needs to be regulated by placing early notification as an obligation of the Processor. Such notification should not wait until all information is complete. Initial information concerning the time of the incident, affected system, type of data involved, suspected cause, and initial mitigation measures is sufficient to assist the Controller in starting the response. Additional information may be provided gradually. This regulation is important so that the Controller is not delayed in fulfilling notification obligations and carrying out recovery. [12]

Termination of processing should also be part of the Data Processing Agreement. After the service relationship ends, the Processor may not continue to store or use Personal Data without a valid legal basis. The agreement needs to determine whether Personal Data must be returned, deleted, or destroyed, including provisions concerning copies, backups, system records, and evidence of implementation.

Thus, the normative model proposed in this article places the Data Processing Agreement as a legal instrument within the compliance system. The agreement not only functions as the basis of a business relationship but also as an instrument to ensure that the obligations of Controllers and Processors can be implemented, supervised, documented, and accounted for. This model also ensures that the contractual relationship does not merely protect the interests of the parties but remains oriented toward the protection of the rights of Personal Data Subjects.

## Conclusion

The regulation of the obligations and responsibilities of Personal Data Controllers and Personal Data Processors under Law Number 27 of 2022 on Personal Data Protection is partially adequate. The regulation has already distinguished the positions of Controllers and Processors, requires Processors to act based on the order of Controllers, extends certain obligations to Processors, requires written approval for the use of other Personal Data Processors, and determines Processor responsibility when processing is carried out outside the order and purpose of the Controller. However, the regulation is not yet fully adequate at the level of contractual relationships and implementation mechanisms. Several gaps remain in relation to documented instructions, due diligence of Processors, minimum clause standards, Processor assistance, audits and evidence of compliance, early notification of Personal Data Protection failures, flow-down of obligations to other Personal Data Processors, deletion or return of Personal Data after the processing relationship ends, and the allocation of internal and external responsibility. Thus, a normative model of a legal compliance system in Data Processing Agreements needs to be structured as a layered model that consists of compliance principles, internal and external compliance parameters, minimum clause standards, and mechanisms for implementation and accountability. Through this model, a Data Processing Agreement does not merely function as a service agreement or confidentiality clause, but as a legal instrument to translate statutory obligations into mechanisms that can be implemented, supervised, proven, and remain oriented toward Personal Data Protection.

## References


1. Valia A, Pantelis CK, Manolis M, Milena P. Retailing in the EU: Policy Actions to Shape a Sustainable, Digital, and Resilient Future. The Economics of Retailing, 2024, 217-168. DOI: https://doi.org/10.1007/978-3-031-72399-5_10
2. Moody RS, Gunardi L, Amad S. Personal Data Protection Law in Indonesia: Challenges and Opportunities. Indonesia Law Review,2024:14(2):175-191.
3. Alfido FAA, Kadek WI. Legal Protection for Digital Illustrators' Data and Copyright to Train Artificial Intelligence-Generated Images. International Journal of Social Science Research and Review,2025:8(12):91-100. DOI: https://doi.org/10.47814/ijssrr.v8i12.3031.

4. Safira WA, Yana SP. Review of Personal Data Protection Legal Regulations in Indonesia. Awang Long Law Review,2022:5(1):280-294. DOI: https://doi.org/10.56301/awl.v5i1.562.
5. Kirk P, Ben M, Matteo M, Richard W, Leyland P. Does (Customer Data) Size Matter? Generating Valuable Customer Insights with Less Customer Relationship Risk. Psychology & Marketing,40(10):2016-2028. DOI: https://doi.org/10.1002/mar.21866Digital [ Object Identifier (DOI)] (https://doi.org/10.1002/mar.21866Digital%20Object%20Identifier%20(DOI)).
6. Deva AS, Habiba SAG, Daffa HND, Shinta H, Muhammad RM. Joint Controllership in the OSS RBA Interoperability System after the Enactment of Indonesia's Personal Data Protection Law. Kertha Patrika,48(1):1-19.
DOI: https://doi.org/10.24843/KP.2026.v48.i01.p01.
7. Reginaldus AJ, Men WW. Perlindungan Hukum bagi Prosesor Data Pribadi dalam Melaksanakan Pemrosesan Data Pribadi Menggunakan Apilikasi Sistem Informasi Kependudukan. Jurnal Pengabdian Masyarakat dan Riset Pendidikan,2026:4(3):19564–19572. DOI: https://doi.org/10.31004/jerkin.v4i3.5184.
8. Indranath G, Sherin SP, Paarth N. Duties and Responsibilities of Controller and Processor. Introduction to Data Protection Law: Cases and Materials from the EU, 2024, 149-186. DOI: https://doi.org/10.1007/978-981-97-6355-9_4.
9. Syahreza F, Sinta DR, Prita A. Protection of Data Subject Rights in the Transfer of Personal Data between Data Controllers in Indonesia: A Comparative Analysis of the PDP Law and the EU GDPR. Awang Long Law Review,2026:8(2):518-529. DOI: https://doi.org/10.56301/awl.v8i2.1827.
10. Ari AP, Angga FA, Grace YS. Kepastian Hukum dalam Transfer Data Lintas Negara: Tinjauan Terhadap Undang-Undang Perlindungan Data Pribadi di Indonesia. Al-Zayn: Jurnal Ilmu Sosial & Hukum,4(2):7838-7851.
11. Moh AH. Tinjauan Yuridis Perlindungan Data Privasi Terhadap Kebocoran Data oleh Instansi Pemerintah. Judge: Jurnal Ilmu Hukum,6(8):1611-1618.
12. Tek RC. Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. In Improving Decision Making Using Semantic Web Technologies. Wiesbaden: Springer Fachmedien Wiesbaden, 2025, 155-212.