Kertha Patrika
P-ISSN 0215-899X E-ISSN 2579-9487

Joint Controllership in the OSS RBA Interoperability System after the Enactment of Indonesia's Personal Data Protection Law

Deva Alfianto Supardi[1], Habiba Salsabil Ananda Ghofar[2], Daffa Hakima Nur Dzaki[3], Shinta Hadiyantina[4], Muhammad Reza Magistra[5]

[1] Faculty of Law University of Brawijaya, Indonesia, email: devaalfianto@student.ub.ac.id
[2] Faculty of Law University of Brawijaya, Indonesia, email: habibasalsabil@student.ub.ac.id
[3] Faculty of Law University of Brawijaya, Indonesia, email: daffahakima@student.ub.ac.id
[4] Faculty of Law University of Brawijaya, Indonesia, email: shinta_fh@ub.ac.id
[5] Master of Law Program Lund University, Sweden, email: reza_magistra@webmail.student.lu.se

Article Info
Submitted: 21-02-2026
Accepted: 07-04-2026
Published: 30-04-2026

Keywords:
Personal Data Protection; Joint Controllership; OSS RBA

Abstrak

Reformasi perizinan berusaha melalui Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja telah melahirkan sistem Online Single Submission Berbasis Risiko (OSS RBA) yang mengandalkan interoperabilitas data secara real-time dari berbagai instansi pemerintah. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memperkenalkan rezim hukum baru yang menciptakan ketidakjelasan status hukum para pihak dalam ekosistem OSS RBA. Penelitian ini bertujuan menganalisis kualifikasi hukum para pihak dalam pemrosesan data pribadi di ekosistem, mengevaluasi penerapan konsep joint controller dalam interoperabilitas OSS RBA, serta merumuskan mekanisme alokasi tanggung jawab hukum jika terjadi kegagalan pelindungan data pribadi. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa relasi antara Kementerian Investasi/Badan Koordinasi Penanaman Modal (BKPM) dan instansi sumber data lebih tepat dikualifikasikan sebagai Pengendali Data Bersama karena mereka secara bersama-sama menentukan tujuan dan sarana pemrosesan data pribadi. Terdapat kekosongan hukum dalam pengaturan joint controllership di OSS RBA. Ketiadaan perjanjian atau regulasi teknis turunan yang mengatur alokasi tanggung jawab menciptakan ketidakjelasan yang dapat merugikan subjek data pribadi. Oleh karena itu, diperlukan regulasi turunan yang mengatur secara detail mekanisme joint controllership dan penegasan kewajiban penyusunan Data Sharing Agreement (DSA) antarinstansi yang mendefinisikan tanggung jawab masing-masing pihak sesuai amanat UU PDP.

Kata kunci:
Pelindungan Data Pribadi; Joint Controllership; OSS RBA

Corresponding Author:
Deva Alfianto Supardi, E-mail: devaalfianto@student.ub.ac.id

DOI:
https://doi.org/10.24843/KP.2026.v48.i01.p01

Abstract

This study analyzes the legal status of actors involved in personal data processing within the OSS RBA ecosystem following the enactment of Indonesia's Personal Data Protection Law (Law No. 27 of 2022). It evaluates whether the relationship between the Ministry of Investment/BKPM and data source agencies should be understood within the framework of joint controllership and examines how legal responsibility should be allocated in the event of personal data protection failures. This research employs a normative legal method using statutory and conceptual approaches. The findings indicate that the relationship between BKPM and data source agencies is best characterized as joint controllership, as both parties jointly determine the purposes and means of processing personal data. However, the current regulatory framework does not clearly regulate joint controllership within the OSS RBA system. The absence of technical regulations and formal data-sharing arrangements creates legal uncertainty regarding responsibility allocation and may undermine the protection of data subjects. Accordingly, derivative regulations are needed to establish a clear framework for joint controllership and to mandate the use of Data Sharing Agreements (DSA) between government agencies.

1. Introduction

Licensing regulations in Indonesia are one of the important issues in the administration of government and public services today. The complexity of licensing procedures previously carried out by the public has been evaluated in order to simplify the licensing process. Simplifying licensing procedures has been a key policy objective of President Joko Widodo's administration for the 2019-2024 term.[1] This was realized in the enactment of Law Number 11 of 2020 concerning Job Creation (hereinafter referred to as the Job Creation Law), which was promulgated on November 2, 2020. Article 6 of the Job Creation Law mandates the implementation of risk-based business licensing. This risk-based business licensing approach differs from previous licensing systems, with simplifications applied to several sectors.[2] The implementation of this licensing system includes regulations on risk-based licensing, norms, standards, procedures, and criteria for risk-based business licensing, as well as business licensing through the Online Single Submission Risk-Based Approach (hereinafter referred to as OSS RBA) system.[3]

OSS RBA has been improved from the previous version of the Business Licensing System, with a business risk assessment system that considers not only capital but also the impact on the environment and society. In OSS RBA, businesses are categorized into four risk

[1] Anton Rosari dkk, "Penyederhanaan Izin Usaha Pasca Undang-Undang Cipta Kerja, Berdasarkan Prinsip Pernanrba Besarnya Resiko Berusaha," *Jurnal Ilmu Hukum, Humaniora, dan Politik (JIHPP). Rev.* 4 (2024): 315.

[2] Bahir Mukhammad, "Pelaksanaan Perizinan Berbasis Risiko Pasca Undang-Undang Cipta Kerja," *Jurnal Nalar KRev.* 1 (2021): 14.

[3] Ropiko Duri dkkd, "Efektivitas *Online Single Submission Risk Based Approach (OSS RBA):* Inovasi Perizinan Usaha Mikro Kecil di Perkotaan," *Jurnal Matra Pembaruan. Rev.* 8 (2024): 104-105.

levels: low, medium-low, medium-high, and high.[4] Moreover, one of the main advantages of this system is its ability to issue a Business Identification Number (NIB) automatically and in real-time through data interoperability from various government agencies. As the administrator of the OSS RBA system, the Ministry of Investment/Investment Coordinating Board (BKPM) retrieves data directly from data source agencies, eliminating the need for applicants to manually submit documents to each relevant agency. The data source agencies connected to the OSS RBA ecosystem include 1) the Directorate General of Population and Civil Registration (Ditjen Dukcapil) of the Ministry of Home Affairs, which is tasked with providing Population Registration Numbers (NIK) and validating the identities of business actors; 2) the Directorate General of Taxes (DJP) of the Ministry of Finance, which is tasked with providing Taxpayer Identification Number (NPWP) data and validating tax status; 3) the Directorate General of General Legal Administration (Ditjen AHU) of the Ministry of Law and Human Rights, which is tasked with providing data on legal entity profiles, deeds of establishment, and the legal status of business entities; and 4) The Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (ATR/BPN), which is tasked with providing land data, Spatial Utilization Conformity (KKPR), and spatial planning information. The interoperability of these data enables faster licensing services, reduces the administrative burden on applicants, and minimizes corruption. However, this massive flow of personal data between agencies also presents new legal risks, especially after the enactment of Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law) on October 17, 2022. The PDP Law introduces a legal regime regarding personal data processing in Indonesia. This law defines various actors in the personal data ecosystem, particularly Personal Data Controllers and Personal Data Processors. The PDP Law also explicitly regulates the obligations of Data Controllers and Data Processors, as well as their legal responsibilities, whether administrative, civil, or criminal, in the event of a failure to protect personal data.

The concept of *joint controllership* is familiar in the international personal data protection regime, particularly in the General Data Protection Regulation (GDPR) of the European Union. Article 26 of the GDPR explicitly states that "*where two or more controllers jointly determine the purposes and means of processing, they are joint controllers*." Article 26 of the GDPR also explicitly regulates the obligation for *joint controllers* to determine their respective responsibilities through transparent arrangements, particularly regarding the implementation of data subjects' rights and their respective obligations to provide information. However, this concept has not been clearly articulated in the PDP Law or its derivative regulations.

The legal uncertainty surrounding the status of parties within the ecosystem has serious legal implications. *First*, uncertainty regarding who is responsible as the Data Controller can lead to *an accountability vacuum* in the event of a personal data protection failure—for example, a leak of NIK and NPWP data from the system. If data is leaked due to *a security vulnerability* in *the Application Programming Interface* (API) of one of the source agencies, who should be held legally responsible? Is it only the agency whose API was hacked? Or is BKPM, as the organizer, also responsible because thesystem stores and processes the data? *Second*, the PDP Law mandates accountability and data protection principles from

[4] Ardita Esti Rahmadani, "Analisis Penerapan Perizinan Berusaha Melalui Sistem *Online Single Submission (OSS)* Berbasis Risiko," *Jurnal Media Hukum Indonesia. Rev.* 2 (2024): 176.

the design stage (*data protection by design and by default*). Article 46 of the PDP Law states *that "in the event of a failure of Personal Data Protection, the Personal Data Controller is obliged to provide written notification no later than 3 x 24 (three times twenty-four) hours to the personal data subject and the institution." T*hese obligations become vague and cannot be effectively enforced without clarity on who is the Data Controller in the system. *Third*, from the perspective of data subjects (business actors who use the system), this ambiguity can harm their rights as guaranteed in the PDP Law, including the right to access, the right to correct inaccurate data, and the right to compensation in the event of a personal data protection failure. *Fourth*, regulations regarding the Electronic-Based Government System (SPBE) as stipulated in Presidential Regulation Number 95 of 2018 concerning the Electronic-Based Government System (Perpres SPBE) mandated the principle of "*data sharing*" between government agencies. However, Perpres SPBE was drafted before the enactment of the PDP Law, so it is not yet fully aligned with PDP Law's concepts of personal data protection. Law, particularly regarding *controllership* and the allocation of responsibilities in public sector's data sharing scheme.

Based on the background described above, this study aims to analyze the legal qualifications of parties involved in personal data processing within the ecosystem, evaluate the application of the *joint controller* concept in OSS RBA interoperability, and formulate a mechanism for allocating legal responsibility in the event of a personal data protection failure.

2. Research Methods

This research adopts a normative legal research approach, using two main approaches: a statutory approach and a conceptual approach.[5] This research also conducts comparative studies with other countries. The legal materials analyzed in this study consist of secondary data, selected based on their relevance to the research objectives, including: (1) primary legal materials, including laws and regulations related to personal data protection, business licensing, and electronic-based government systems comprising statutes and regulations related to personal data protection, business licensing, and electronic-based government systems, particularly Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2020 concerning Job Creation, and their implementing regulationss; (2) secondary legal materials, including textbooks, law journals, scientific articles, and legal doctrines; and (3) tertiary legal materials, including legal dictionaries and legal encyclopedias. The techniques used to collect legal materials included library research and documentation study. Legal analysis is conducted using qualitative normative techniques, including systematic interpretation, legal reasoning, and doctrinal analysis.

3. Results and Discussion

3.1. Legal Qualification of the Parties in Personal Data Processing within the OSS RBA Ecosystem

The PDP Law defines the actors in the personal data protection ecosystem ecosystem. Article 1 point 6 of the PDP Law defines a Personal Data Controller (Controller) as any

[5] Marzuki, Mahmud. Penelitian hukum: Edisi revisi. Prenada Media, 2017.

person, public agency, and international organization acting alone or jointly in determining the purpose and exercising control over Personal Data Processing. Meanwhile, Article 1 point 7 of the PDP Law defines a Personal Data Processor as any person, public agency, and international organization acting alone or jointly in performing personal data processing on behalf of a Controller".

From the above definition, there are elements that distinguish between Controllers and Personal Data Processors. Controllers are the parties who determine the purposes and means of processing personal data. They are parties that have the authority to decide what the data is processed for and how the data is processed. Meanwhile, a Personal Data Processor is a party that processes personal data on behalf of a Controller.[6] A Personal Data Processor does not have the authority to determine the purpose of processing, but only carries out instructions from the Controller. The fundamental difference lies in who determines the purpose and control of processing and who performs the processing based on those instructions.

This *definition* a closely mirrors the concepts of data controller and data processor in the GDPR. Article 4(7) of the General Data Protection Regulation defines *a data controller* as "*the natural or legal person... which, alone or jointly with others, determines the purposes and means of the processing of personal data*". Meanwhile, Article 4(8) of the GDPR defines a data processor as "*a natural or legal person... who processes personal data on behalf of the controller*" or, loosely translated, "*a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the data controller*". Adopting this comparative lens is useful given that the PDP Law was substantially informed by the GDPR architecture.

OSS RBA has been integrated with several Ministry systems from data source agencies such as the Directorate General of Population and Civil Registration (Ditjen Dukcapil), the Directorate General of Taxes (DJP), and the Directorate General of General Legal Administration (Ditjen AHU). These agencies play an important role as data owners and managers. Their legal qualification as Controllers is analyzed separately below.

The Directorate General of Population and Civil Registration (Ditjen Dukcapil) is responsible for collecting, storing, and managing population data for the purposes of population administration, elections, and other public services in accordance with Law Number 24 of 2013 concerning Population Administration. Article 584 of Regulation of the Minister of Home Affairs of the Republic of Indonesia Number 137 of 2022 reiterates *that "the Directorate General of Population and Civil Registration has the task of formulating and implementing policies in the field of population and civil registration in accordance with the provisions of laws and regulations*". Because Ditjen Dukcapil independently establishes both the purpose of population data collection and the technical conditions under which such data may be accessed by external systems, it satisfies both constitutive elements of the Controller definition under Article 1(6) of the PDP Law. Accordingly, Ditjen Dukcapil is appropriately qualified as a Controller with respect to population master data.[7]

---

[6] Haris Satiadi, "Perbedaan Pengendali dan Prosesor Data Pribadi Menurut UU PDP," *Hukum Online.* (2022): https://www.hukumonline.com/klinik/a/perbedaan-pengendali-dan-prosesor-data-pribadi-menurut-uu-pdp-lt636d1861766bc

[7] Pasal 584 Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 137 Tahun 2022 tentang Tentang Organisasi dan Tata Kerja Kementerian Dalam Negeri

The Directorate General of Taxes (DJP) is responsible for collecting and managing tax data for the purposes of tax collection, monitoring taxpayer compliance, and enforcing tax laws in accordance with Law No. 6 of 1983 concerning General Provisions and Tax Procedures, as amended several times, most recently by the Job Creation Law. DJP independently determines the legal basis and operational procedures governing the sharing of tax identification data with the OSS RBA system pursuant to its own sectoral mandate, rather than under instruction from any other agency. Accordingly, DJP qualifies as a Controller for tax-related personal data.

The Directorate General of General Legal Administration (Ditjen AHU) is tasked with collecting and managing legal entity data (articles of association, bylaws, management structure, etc.) for the purposes of registration and supervision of legal entities in accordance with Law Number 40 of 2007 concerning Limited Liability Companies and related regulations. Ditjen AHU autonomously determines the scope, purpose, and technical procedures of data processing within its legal administration system, thereby qualifying Ditjen AHU as a Controller for legal entity master data within the meaning of the PDP Law.

From this description, the data source agencies meet the criteria as Controllers for the master data they collect and manage. Independently, the data source agencies determine the purpose of data collection and the means of data processing. This authority stems from sectoral laws and regulations that mandate each agency.

The Ministry of Investment/BKPM is an Indonesian government agency that connects all investment sectors from technical ministries. The Ministry of Investment/BKPM connects business actors with the government to create a conducive investment climate.[8] The Ministry of Investment/BKPM uses data obtained from source agencies to verify and issue NIBs as the system administrator. NIBs serve as official identities for business actors and provide various benefits, such as access to financing, legal protection, and ease in establishing cooperation with other parties.[9]

According to Article 13 paragraph (1) letter a of the Regulation of the Minister of Investment and Downstream Industry/Head of the Investment Coordinating Board Number 7 of 2025 concerning Data Governance of the Ministry of Investment and Downstream Industry/BKPM (Permen BKPM 7/2025) states that Data Producers within the Ministry of Investment/BKPM are tasked *with "producing data by collecting, compiling, processing, and updating Data in accordance with the principles of One Data Indonesia within their respective scopes and fields of duty and in coordination with the Investment Coordinator and/or Data Manager."* In the context of investment, the Ministry of Investment/BKPM plays a role in determining new objectives in the processing of such data, namely for the purposes of business licensing.Based on Government Regulation Number 28 of 2025 concerning the Implementation of Risk-Based Business Licensing (PP 28/2025), the BKPM

[8] Riyan Latifahul Hasanah dan Prisilia Semestanti, "Pengaruh Kualitas Terhadap Kepuasan Pengguna Website OSS Kementerian Investasi Menggunakan Metode Webqual 4.0," *Jusifor: Jurnal Sistem Informasi dan Informatika. Rev.* 3 (2024): 29.

[9] Muhammad Firdaus Al Faaiz, "Pelatihan Pembuatan Legalitas Usaha NIB Secara Mandiri dan Sertifikasi Halal Sebagai Sarana Meningkatkan Kredibilitas Usaha Mahasiswa di Surabaya," *IMPACT: Jurnal Pengabdian Kepada Masyarakat. Rev.* 1 (2025): 16.

coordinates the implementation of risk-based business licensing across agencies,[10] receiving applications for the acquisition or submission of business licenses based on business activities,[11] The Ministry of Investment/BKPM has the authority to propose the implementation schedule and inspection personel into the system as the implementer of routine field inspections.[12] In addition, BKPM Regulation 7/2025, which is the implementing regulation of PP 28/2025, specifically regulates the mechanism for data exchange and dissemination between agencies, including the use of electronic systems and data interoperability.[13]

The relationship between the Ministry of Investment/BKPM and data source agencies cannot be adequately explained using a single Controller-Processor model. If BKPM is considered a Personal Data Processor working on behalf of the source agency, this indicates an inconsistency. This is because the Ministry of Investment/BKPM has independent authority to determine the purpose of data processing (such as issuing NIBs), which differs from the original purpose of data collection of the source agency. Conversely, if BKPM is considered the sole Controller for all data processed in the system, there is an inconsistency because the Ministry of Investment/BKPM does not have the authority to collect data directly from data subjects, but only receives data from source agencies that have the authority to collect data based on sectoral laws. Thus, a more precise legal construct is needed. Which, as will be elaborated in the discussion that follows, is the concept of joint controllership under Article 1(9) of the PDP Law.

In the development of legal doctrine and research prior to the enactment of the PDP Law, the relationship between the Ministry of Investment/BKPM, OSS institutions, and data source agencies was analyzed more from the perspective of electronic system operators than through the categories of Personal Data Controllers and Processors. Twotik Lestariningtyas, for example, points out that neither OSS 1.1 nor OSS RBA provide explicit regulations regarding the protection of personal data of system users, so that such protection is derived from the regime of Law Number 1 of 2024 concerning the Second Amendment to LawLaw Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP 71/2019), Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems (PP 80/2019), and Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection in Electronic Systems (Permenkominfo 20/2016).[14] With this framework, OSS institutions are classified as electronic system operators that are obliged to maintain data confidentiality and are responsible in the event of a data breach, while the Ministry of Investment/BKPM and data source agencies are positioned as parties that obtain access rights and utilize data within the framework of business licensing. The enactment of the PDP Law shifts the focus

[10] Pasal 6 ayat (2) Peraturan Pemerintah Nomor 28 Tahun 2025

[11] Pasal 8 ayat (2) dan (4) Peraturan Pemerintah Nomor 28 Tahun 2025

[12] Pasal 244 ayat (5) huruf b dan c Peraturan Pemerintah Nomor 28 Tahun 2025

[13] Pasal 22 ayat (2) dan (3) Permen 7/2025 Peraturan Menteri Investasi dan Hilirisasi/Kepala BKPM Nomor 7 Tahun 2025

[14] Twotik Lestariningtyas, "Perlindungan Data Pribadi Pengguna Sistem Layanan Perizinan Berusaha Terintegrasi Secara Elektronik OSS 1.1 dan OSS RBA (*Risk Basic Approach*)," Jurnal Jendela Hukum, hlm. 30–32.

of analysis because the categories of Personal Data Controllers and Personal Data Processors are now the main reference for determining who bears legal responsibility for the design, decisions, and risks of data processing in OSS RBA.

Similar lessons can be drawn from the *Open Application Programming Interface (API) Payment* ecosystem, which also relies on the interoperability of electronic systems and cross-stakeholder *data sharing* practices. Research by Pinky Eskah Prayoga and R.A. Antari Inaka Turingsih shows that in *Open API Payment*, personal data protection arrangements cannot rely solely on the consent of the data subject, but must be supplemented by a written agreement that details the roles and responsibilities of data controllers, *data users*, and other personal data processors, and is supported by supervisory authorities' effective oversight mechanisms.[15] This legal relationship configuration confirms that when several entities jointly determine the purposes and means of processing, their relationship tends to qualify as *joint controllers*. Meanwhile, other parties that only process data based on the controllers' mandate are positioned as processors. The pattern of data interconnection in OSS RBA has similar characteristics because it involves data source agencies and the Ministry of Investment/BKPM, each of which has a degree of determination regarding the purpose of processing (whether for the purposes of population administration, taxation, or business licensing). Thus, the legal qualification of the Ministry of Investment/BKPM and data source agencies as Personal Data Controllers, either separately or jointly, becomes the starting point for designing proportional contractual arrangements and data governance in the OSS RBA ecosystem, which will be further elaborated in the discussion on the concept of *joint controllership*.

3.2. The Concept of Joint Controllership in Interoperability

Article 1 point 6 of the PDP Law explicitly states that a Controller is a party that "*acts alone or jointly in determining the purpose and exercising control over the Processing of Personal Data*." The phrase "acting... jointly" indicates that the PDP Law recognizes the possibility of more than one Controller being jointly responsible for the processing of personal data. This concept is known as *Joint Controller*. Although the PDP Law does not provide a definition of *joint controllership*, the recognition of the possibility of "acting jointly" in determining the purposes and means of personal data processing provides a legal basis for the application of this concept in Indonesia.

In the GDPR, the concept *of joint controllership* is regulated in more detail in Article 26, entitled "Joint Controllers." Article 26(1) of the GDPR states:

"*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 and duties 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...*"

Based on Article 26 of the GDPR states three key elements in *joint controllership*: 1) Joint Determination of Purposes and Means: Two or more parties jointly determine the

[15] Pinky Eskah Prayoga dan R.A. Antari Inaka Turingsih, "Pelindungan Data Pribadi dalam Open Application Programming Interface (Open API) Payment: Studi Komparatif Inggris dan Indonesia," Viva Justicia: Journal of Private Law 1, no. 2 (2025): 243–266.

purposes and means of processing personal data. This joint determination does not have to be made through a formal agreement, but can also occur through factual cooperation or joint decisions. *Joint controllers* have joint responsibility for GDPR compliance. However, this responsibility can be allocated differently among the parties through internal arrangements. *Joint controllers* are then required to transparently determine each party's responsibilities, particularly regarding the exercise of data subjects' rights and the obligation to provide information.

CJEU case C-210/16 Wirtschaftsakademie has provided interpretations regarding joint controllership in several important cases. In the Wirtschaftsakademie Schleswig-Holstein case (C-210/16)[16], the judgment ruled that the administrator of *the Facebook Fanpage* and Facebook Ireland Ltd. were *joint controllers* because both parties jointly determined the purposes and means of processing visitor data on the page. In the C-40/17 Fashion ID (C-40/17)[17], the judgment established that *joint controllership* can apply even if the parties have different levels of responsibility or are involved in different processing stages. The principle that can be drawn from the judgment rulings is that the determination of the purposes and means of processing does not have to be done entirely jointly or with the same intensity. It is sufficient that two parties have *common influence* or *common decision* over certain aspects of the processing of personal data to qualify as *joint controllers*.

The relationship between BKPM and data source agencies in the ecosystem can be considered joint controllership based on the following reasons:

1) There is a joint determination of the purpose of data processing. Although the data source agencies collect data for their own initial purposes, data sharing with thesystem for issuing NIBs is a new purpose jointly determined by the data source agencies and BKPM. This data sharing is based on Government Regulation No. 28 of 2025 and Presidential RegulationNo. 95 of 2018 concerning Electronic-Based Government Systems. The source agencies also give their approval and implement data interoperability because they also have an interest in accelerating business licensing as part of government bureaucratic reform.
2) Joint determination of the data processing tools. Data interoperability in the system requires technical cooperation between BKPM and source agencies in determining data processing tools, including: a) Data exchange protocols through API (Application Programming Interface); b) Data formats and standards to be shared; c) Data access authentication and authorization mechanisms; d) Data security procedures; and e) Data pulling frequency and timing. These technical means cannot be determined unilaterally by BKPM or the source agency, but they require coordination and mutual agreement. Thus, there is joint influence in determining the means of data processing.
3) Shared responsibility for data security. Both BKPM and the source agency are responsible for the security of the personal data being processed. BKPM is responsible

[16] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, Judgment of the Court (Grand Chamber), 5 June 2018, ECLI:EU:C:2018:388, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62016CJ0210.

[17] *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, C-40/17, Judgment of the Court (Second Chamber), 29 July 2019, ECLI:EU:C:2019:629, https://curia.europa.eu/juris/liste.jsf?num=C-40/17.

for data security in the system and protection against unauthorized access, whereas the source agency is responsible for data security in their system and the security of the API they provide. From a legal perspective, a shared responsibility that cannot be clearly separated.

4) Joint regulatory basis for data processing. The data interoperability between BKPM and source agencies is not a voluntary or ad hoc arrangement but is mandated by Government Regulation No. 28 of 2025 and Presidential Regulation No. 95 of 2018, both of which impose obligations on all participating agencies to share data within the OSS RBA framework. This shared regulatory obligation demonstrates that each agency exercises joint authority in shaping the overall data processing architecture. There is also a shared institutional interest in accelerating business licensing and advancing bureaucratic reform, which further reinforces the characterization of their relationship as joint controllership under Article 1(9) of the PDP Law.

Provisions regarding joint controllers can also be found in Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System. This Presidential Regulation on SPBE regulates Data Sharing in Chapter V. Article 41 of the Presidential Regulation on SPBE states that :

> "*(1) Data sharing between central and regional agencies shall be carried out with due regard to the principles of security, confidentiality, and integrity of data. (2) Data sharing as referred to in paragraph (1) shall be carried out through the Government Service Connection System.*"

Then, Article 42 of the Presidential Regulation on SPBE regulates Data Owners and Data Users as follows:

> "*(1) Data Owners are responsible for the accuracy, quality, and security of the Data they manage. (2) Data Users are responsible for maintaining the confidentiality and security of the Data obtained from Data Owners.*"

The concepts of "Data Owner" and "Data User" in the SPBE Presidential Regulation are not in line with the concepts of Controller" and " Personal Data Processor" in the PDP Law, given that Perpres SPBE was drafted before the PDP Law came into effect. Several inconsistencies can be identified: (1) the absence of the concept of joint controllership; (2) the absence of a Data Sharing Agreement obligation; and (3) the absence of data subject rights protection in the data sharing mechanism. With the enactment of the PDP Law, there is an urgent need to revise Perpres SPBE or to issue derivative regulations that specifically govern the mechanism for data sharing in the public sector based on the principle of joint controllership.

With the enactment of the PDP Law, there is an urgent need to revise the Presidential Regulation on SPBE or issue derivative regulations of the PDP Law that specifically regulate the mechanism for data sharing in the public sector based on the principle *of joint controllership*.

3.2. Allocation of Legal Responsibility

Under the PDP Law, the starting point for the allocation of legal responsibility is the principle that the Personal Data Controller bears primary responsibility for all personal data processing activities under its control, including processing that is actually carried

out by another party on behalf of the Controller.[18] Article 46 of the PDP Law regulates the Controller's duty to ensure lawful, accurate, secure, and purpose-specific processing, while Article 51 emphasizes that the Personal Data Processor is liable if it processes data outside of the Controller's instructions or beyond the purposes specified by the Controller.[19] In a joint controllership arrangement, each controller may be held jointly and severally liable for damage suffered by the data subject. Thus, the existence of more than one controller should not reduce the guarantee of protection for personal data subjects, as each Controller remains fundamentally liable for any violations that occur as long as they remain within the scope of the processing they control.

In the context of OSS RBA, data source agencies such as the Directorate General of Population and Civil Registration (Ditjen Dukcapil), the Directorate General of Taxes, and the Directorate General of General Legal Administration (Ditjen AHU) bear primary responsibility for the legal basis of data collection, the accuracy and timeliness of master data, and compliance with the principle of purpose limitation in accordance with their respective sectoral mandates. In the event of identity errors, outdated legal entity status data, or tax data discrepancies that result in losses for business actors, the source agency as the master data controller has the primary responsibility, as they determine the purpose of collection and the means of processing in the sectoral database. As the Personal Data Controller in the OSS RBA ecosystem, the Ministry of Investment/BKPM is responsible for designing the system architecture, regulating interoperability, determining licensing risk profiles, and ensuring the security of processing when personal data from various source agencies is integrated and used for the NIB verification and issuance process.[20] In the event of a data breach, unauthorized access, or misuse of user credentials within the OSS RBA , the primary responsibility shifts to BKPM as the Controller of the processing activities that occur within the system, without prejudice to the possibility of recourse against other parties who fail to meet security standards or contractual obligations.

This allocation of responsibilities should ideally be based not only on the general norms of the PDP Law but also on derivative regulatory instruments and agreements between controllers. Research on personal data protection in OSS shows that prior to the enactment of the PDP Law, the obligations of OSS operators were mostly formulated from the perspective of electronic system operators, so that responsibilities were understood as limited to the obligation to maintain data confidentiality and security based on the ITE Law, PP 71/2019, and Permenkominfo 20/2016. After the PDP Law came into effect, the regulatory basis shifted to the Controller-Processor regime, so that the relationship between BKPM and the source agency must be translated into a Data Sharing Agreement (DSA) that details the obligations related to the basis of processing, security, recording of processing activities, incident handling, and fulfillment of data subject rights. Experience in other sectors, such as Open API Payment, shows that the

[18] Pasal 1 angka 6 dan Pasal 46 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

[19] Pasal 51 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

[20] Peraturan Pemerintah Republik Indonesia Nomor 28 Tahun 2025 tentang Perizinan Berusaha Berbasis Risiko; Peraturan Menteri Investasi dan Hilirisasi/Kepala Badan Koordinasi Penanaman Modal Nomor 7 Tahun 2025 tentang Tata Kelola Data Kementerian Investasi dan Hilirisasi/Badan Koordinasi Penanaman Modal.

division of roles and responsibilities between controllers and data users, which is only outlined globally in sectoral regulations, is insufficient; concrete contractual arrangements and oversight mechanisms that ensure collective accountability are needed.[21] In line with this, the idea of data protection by design and by default highlighted by Hadiyantina et al. in the context of medical records is also relevant to OSS RBA: from the system design and interoperability scheme stages, BKPM and source agencies must design a clear, proportional, and documented allocation of responsibilities so that there is no "passing of responsibility" when the rights of personal data subjects are violated.[22]

3.2.1. Legal Obligations of Controllers and Processors of Personal Data in the PDP Law

Article 46 of the PDP Law regulates the obligations that must be fulfilled by Personal Data Controllers, which include:

a. ensuring the accuracy, completeness, non-misleading nature, up-to-date status, and accountability of Personal Data in relation to the purposes of Personal Data Processing;

b. protecting and ensuring the security of Personal Data obtained and under their control by taking into account applicable technical and organizational standards;

c. preventing Personal Data Protection failures, including leaks, damage, or loss of Personal Data:

d. notify the Subject of Personal Data and the Institution in writing within a maximum of 3 x 24 (three times twenty-four) hours after becoming aware of the occurrence of a Personal Data Protection failure as referred to in letter c that poses a high risk to the personal interests of the Subject of Personal Data;

e. take the necessary steps to remedy the Personal Data Protection failure as referred to in letter c;

f. provide compensation and/or damages to the Personal Data Subject who has suffered losses due to the Personal Data Protection failure; and

g. notify the Data Subject in writing of the efforts made to address the Personal Data Protection failure that has occurred.

The above obligations are imperative and constitute the data controller accountability principle. Violations of these obligations may result in administrative, civil, or criminal sanctions. Article 51 of the PDP Law regulates the obligations of Personal Data Processors:

a. to process Personal Data in accordance with the Personal Data Controller's written instructions, unless otherwise specified by statutory provisions;
b. ensuring that any person acting under the authority of the Personal Data Processor who has access to Personal Data does not process Personal Data, unless

[21] Pinky Eskah Prayoga dan R.A. Antari Inaka Turingsih, op. cit.,
[22] Hadiyantina, Shinta, Zainal Amin Ayub, Dewi Cahyandari, Amelia Ayu Paramitha, Sinta Devi Ambarwati, Yusuf Mustofa, Xaviera Qatrunnada Djana Sudjati, and Nur Auliya Rahmatika. Perlindungan Data Pribadi Dalam Bidang Rekam Medis. Universitas Brawijaya Press, 2023.

instructed by the Personal Data Controller or required by the provisions of laws and regulations;

c. protect and ensure the security of Personal Data obtained and under its control by observing applicable technical and organizational standards; and
d. return or destroy Personal Data in accordance with the written instructions of the Personal Data Controller or the provisions of laws and regulations after the completion of Personal Data Processing.

Although the Data Processor has certain obligations, the primary responsibility for the protection of personal data remains with the Data Controller. The Data Processor is responsible in the context of performing the instructions of the Data Controller.

3.2.2. Implications of Joint Controllership on Responsibilities

If BKPM and data source agencies are classified as *Joint Controllers*, then the legal responsibility for failure to protect personal data in the system becomes *joint and several liability*. That said, the PDP Law does not explicitly regulate the mechanism for allocating responsibility among *joint controllers*. In the GDPR, Article 26(3) stipulates that data subjects may exercise their rights against each *joint controller*, and Article 82(4) stipulates *joint and several* liability in the context of compensation for damages:

> "*Where more than one controller or processor, or both a controller and a processor, are involved in the same processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.*"

Or, if translated freely, it means:

> "*Where more than one controller or processor, or a combination of controllers and processors, is involved in the same processing, each controller or processor shall be liable for the entire loss in order to ensure effective compensation for the data subject.*"

However, Article 82(5) also provides a *right of recourse*:

> "*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 compensation corresponding to their part of responsibility for the damage...*"

Or, if translated freely, it means:

> "*If a controller or processor, in accordance with paragraph (4), has paid full compensation for the loss suffered, that controller or processor has the right to reclaim from other controllers or processors involved in the same processing the portion of compensation corresponding to their share of responsibility for the loss...*"

In the absence of similar provisions in the PDP Law, *a legal* vacuum exists regarding the mechanism for allocating responsibility among *joint controllers* in Indonesia.

To understand the implications of unclear responsibility allocation, two possible scenarios of data leaks in the system. First, if the data leak is due to a security breach in the API of the Directorate General of Population and Civil Registration. Suppose there

is a leak of 1 million business owners' NIK, names, and addresses due to *a security vulnerability* in the API provided by the Directorate General of Population and Civil Registration for the system. Hackers exploit this security vulnerability and download the datThen, the leaked data is misused for *identity fraud. The following legal questions arise in this scenario:* 1) Is the Directorate General of Population and Civil Registration solely responsible for the security vulnerability is in their system? 2) Or is the Investment Coordinating Board (BKPM) also responsible because thesystem collects and stores the data, thereby having an obligation to ensure that the data it receives comes from a secure source? 3) Can other source agencies (Directorate General of Taxes, the Directorate General of Administrative Affairs) also be held collectively responsible as part of an ecosystem that failed to protect personal data?

Based on the concept *of joint controllership*, the Directorate General of Civil Registration and the Investment Coordinating Board can be held accountable because they jointly determine the purpose and means of data processing. The Directorate General of Civil Registration has direct responsibility for the security of the API they provide, while the Investment Coordinating Board has the responsibility to ensure that adequate security standards are followed for data interoperability. That said, without a *Data Sharing Agreement* (DSA) that regulates the responsibilities of each party in detail, determining the proportion of responsibility becomes very difficult and can cause disputes between agencies.

Second, if data leakage occurs due to a *ransomware* attack on the server. Suppose that the system managed by BKPM becomes the target of a *ransomware* attack that successfully encrypts the entire business licensing database, including NIK, NPWP, and legal entity information stored in the system. Hackers demand a ransom of millions of dollars and threaten to publish the data if the ransom is not paid. In this scenario, the following questions arise: 1) Is BKPM solely responsible because the attack occurred on their server? 2) Or are the data source agencies also responsible because they provided data to a system that did not have adequate security protection against *ransomware* attacks? 3) Do source agencies have an obligation to conduct security audits ofsystems before providing data access? Based on the concept *of joint controllership* , responsibility can be shared between BKPM, which failed to protect the data in the system, and the source agency, which provided data to a system that did not have adequate security *due diligence*. However, once again, the absence of a DSA regulating each party's obligations creates legal uncertainty. Data subjects who have suffered losses face difficulties in determining which party they should file a claim for compensation.

3.2.3. The Principle of Strict Liability in Personal Data Protection Failures

The PDP Law adopts the principle of *strict liability* in several contexts of personal data protection failures. Article 46 paragraph (1) letter f requires Personal Data Controllers to "*provide compensation and/or damages to Personal Data Subjects who suffer losses due to Personal Data Protection failures*" without requiring any element of fault on the part of the Data Controller. This *strict liability* principle is in line with the global trend in personal data protection, which places a high burden of responsibility on parties that manage personal data. However, in the context *of joint controllership*, the application *of strict liability* becomes more complex due to the difficulty of determining the responsible party. If there are multiple *joint controllers*, personal data subjects may find it difficult to

determine to which party they should file a compensation claim. Then there is the potential for *forum shopping*. Personal data subjects may choose to sue the *joint controller* with the greatest financial capacity or the one that is "easiest" to sue, even though their contribution to the data protection failure may be smaller. Finally, without a clear recourse mechanism, *joint controllers* who pay full compensation to data subjects have no strong legal basis to claim contributions from other *joint controllers* in proportion to their respective responsibilities.

From a historical perspective, the application of the principle of almost absolute responsibility for the failure to protect personal data in the OSS RBA must also be seen as a correction to the data protection regime prior to the enactment of the PDP Law. A number of studies on the early generation of OSS (PP 24/2018) show that the design of personal data protection in the OSS environment is basically only supported by the general norms of the ITE Law, PP 71 of 2019, and Permenkominfo 20 of 2016, without explicit regulations regarding personal data protection guarantees or legal consequences in the event of a data breach. Hasbi Pratama, for example, emphasized that PP 24/2018 does not contain explicit obligations for OSS Institutions to guarantee the protection of business actors' personal data, so that normatively there is a possibility of data leaks without clear mechanisms of accountability and compensation for the injured party. These findings reveal a regulatory gap that is now filled by the PDP Law through the introduction of compensation obligations for Personal Data Controllers, but at the same time raises new questions about how the principle of strict liability should be distributed among data controllers in a joint controllership configuration such as OSS RBA.

Normative experience in the OSS sector prior to the PDP Law, as well as comparisons with other sector regimes, indicate that the principle of strict liability cannot be allowed to operate alone without the support of a clear governance design among joint controllers. Research on personal data protection in OSS 1.1 and OSS RBA shows that so far, responsibility has tended to be attached abstractly to "electronic system operators," without detailed distinctions between the obligations of each entity that controls and utilizes data. On the other hand, studies on Open API Payment emphasize the importance of written agreements that explicitly divide roles, responsibilities, and recourse mechanisms between controllers and other parties that process data, so that the burden of responsibility does not fall disproportionately on the single financially strongest actor. In the context of OSS RBA, this means that the PDP Law needs to be supported by derivative regulations and Data Sharing Agreements between the Ministry of Investment/BKPM and data source agencies that: (a) determine who is the primary contact for data subjects when claiming compensation; (b) regulate recourse rights and the sharing of compensation based on the degree of contribution to the failure of protection; and (c) integrate the principles of data protection by design and by default into the technical and contractual architecture, so that the risks of forum shopping and "passing the buck" can be minimized. Thus, the principle of strict liability in Article 46 paragraph (1) letter f of the PDP Law serves not only as a threat of sanctions, but also as a driving force for data controllers to design a transparent and accountable responsibility allocation scheme from the outset in the OSS RBA ecosystem.

3.2.4. Implications for Data Subject Rights

The lack of clarity in the allocation of responsibilities in joint controllership also has an impact on the exercise of data subject rights as guaranteed in Article 5 of the PDP Law, which includes:

1. The right to obtain information about the Data Controller processing their personal data;
2. The right to access Personal Data being processed;
3. The right to request correction of inaccurate Personal Data;
4. The right to demand the deletion of Personal Data under certain conditions;
5. The right to obtain compensation for failure to protect personal data.

If data subjects wish to exercise the above rights in relation to their personal data processed in the OSS RBA system, to whom should they submit their requests? Should they submit them to the Ministry of Investment/BKPM, to the data source agency, or to both? The exercise of data subjects' rights becomes ineffective without clarity regarding the point of contact and responsibilities' allocation.

4. Conclusion

First, the relationship between BKPM and data source agencies in the OSS RBA ecosystem is best understood as joint controllership. Data source agencies exercise independent authority over the purposes and means of their respective master data pursuant to sectoral legal mandates, while BKPM determines new processing purposes through the OSS RBA system. Their relationship reflects an equal, horizontal arrangement of joint Controllers rather than a vertical Controller-Processor hierarchy.

Second, a significant legal void persists in the regulation of joint controllership within the OSS RBA ecosystem. In this context, the absence of a Data Sharing Agreement (DSA) or derivative technical regulations governing the allocation of responsibility among Controllers creates uncertainty that directly undermines the rights of data subjects under Article 5 of the PDP Law.

Third, to address this legal void, derivative regulations are needed to govern joint controllership mechanisms in the Electronic-Based Government System (SPBE). Concretely, this includes: (1) a mandatory requirement for a Data Sharing Agreement (DSA) between BKPM and each data source agency, clearly defining each party's obligations and liability allocation; and (2) revision of Presidential Regulation No. 95 of 2018 on SPBE to align its data-sharing framework with the Controller and Processor definitions established by the PDP Law. The PDP Law does not explicitly regulate (a) joint and several liability; (b) recourse mechanisms for joint controllers who have paid full compensation; (c) the proportion of liability based on contribution to the failure of data protection; and (d) a point of contact for data subjects. The absence of these mechanisms creates a situation that is detrimental to personal data subjects and may give rise to disputes between government agencies in the future.

Reference

Agung, Hasbi Pratama Arya. "Perlindungan Data Pribadi Dalam Proses Pengurusan Perizinan Perusahaan Berbasis Elektronik Online Single Submission (OSS)." Jurnal Ilmiah Galuh Justisi 9, no. 1 (2021)

Anton Rosari dkk, "Penyederhanaan Izin Usaha Pasca Undang-Undang Cipta Kerja, Berdasarkan Prinsip Perizinan Berbasis Besarnya Resiko Berusaha," Jurnal Ilmu Hukum, Humaniora, dan Politik (JIHPP). Rev. 4 (2024)

Ardita Esti Rahmadani, "Analisis Penerapan Perizinan Berusaha Melalui Sistem Online Single Submission () Berbasis Risiko," Jurnal Media Hukum Indonesia. Rev. 2 (2024)

Bahir Mukhammad, "Pelaksanaan Perizinan Berbasis Risiko Pasca Undang-Undang Cipta Kerja," Jurnal Nalar Keadilan. Rev. 1 (2021)

Dharmawan, Ni Ketut Supasti. "Protecting Traditional Balinese Weaving Trough Copyright Law: Is It Appropriate?" *Diponegoro Law Review* 2, no. 1 (2017): 57–84. https://doi.org/10.14710/dilrev.2.1.2017.57-84.

Diantha, I Made Pasek, and MS Sh. *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum*. Prenada Media, 2016.

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, C-40/17, Judgment of the Court (Second Chamber), 29 July 2019, ECLI:EU:C:2019:629, https://curia.europa.eu/juris/liste.jsf?num=C-40/17.

Hadiyantina, Shinta, Zainal Amin Ayub, Dewi Cahyandari, Amelia Ayu Paramitha, Sinta Devi Ambarwati, Yusuf Mustofa, Xaviera Qatrunnada Djana Sudjati, and Nur Auliya Rahmatika. Perlindungan Data Pribadi Dalam Bidang Rekam Medis. Universitas Brawijaya Press, 2023.

Haris Satiadi, "Perbedaan Pengendali dan Prosesor Data Pribadi Menurut UU PDP," *Hukum Online.* (2022): https://www.hukumonline.com/klinik/a/perbedaan-pengendali-dan-prosesor-data-pribadi-menurut-uu-pdp-lt636d1861766bc

Lestariningtyas, Twotik, and Muhammad Roqib. "Perlindungan data pribadi pengguna sistem layanan perizinan berusaha terintegrasi secara elektronik OSS 1.1 dan OSS RBA (Risk Basic Approach)." Jurnal Jendela Hukum 8, no. 2 (2021): 25-34.

Marzuki, Mahmud. Penelitian hukum: Edisi revisi. Prenada Media, 2017.

Muhammad Firdaus Al Faaiz, "Pelatihan Pembuatan Legalitas Usaha NIB Secara Mandiri dan Sertifikasi Halal Sebagai Sarana Meningkatkan Kredibilitas Usaha Mahasiswa di Surabaya," *IMPACT: Jurnal Pengabdian Kepada Masyarakat. Rev.* 1 (2025)

Prayoga, Pinky Eskah, and RA Antari Inaka Turingsih. "Pelindungan Data Pribadi Dalam Open Application Programming Interface (OPEN API) Payment: Studi Komparatif Inggris dan Indonesia." Viva Justicia: Journal of Private Law 1, no. 2 (2025): 22-45.

Riyan Latifahul Hasanah dan Prisilia Semestanti, "Pengaruh Kualitas Terhadap Kepuasan Pengguna Website OSS Kementerian Investasi Menggunakan Metode Webqual 4.0," *Jusifor: Jurnal Sistem Informasi dan Informatika. Rev.* 3 (2024)

Ropiko Duri dkk, "Efektivitas Online Single Submission Risk Based Approach (RBA): Inovasi Perizinan Usaha Mikro Kecil di Perkotaan," Jurnal Matra Pembaruan. Rev. 8 (2024): 104-105.

Salain, Made Suksma Prijandhini Devi, and I Palguna. "The Regulation of the Ownership of Flats by Foreigners after the Enactment of the Job Creation Law." *Indon. L. Rev.* 12 (2022): 1.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, Judgment of the Court (Grand Chamber), 5 June 2018, ECLI:EU:C:2018:388, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62016CJ0210.

Laws and Regulations

Peraturan Menteri Investasi dan Hilirisasi/Kepala Badan Koordinasi Penanaman Modal Nomor 7 Tahun 2025 tentang Tata Kelola Data Kementerian Investasi dan Hilirisasi/BKPM

Peraturan Pemerintah Nomor 28 Tahun 2025 tentang Penyelenggaraan Perizinan Berusaha Berbasis Risiko, (Lembaran Negara Tahun 2025 Nomor 98, Tambahan Lembaran Negara Nomor 7115).

Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

Undang-undang Nomor 11 Tahun 2020 tentang Cipta Kerja, (Lembaran Negara Tahun 2020 Nomor 245, Tambahan Lembaran Negara Nomor 6573).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, (Lembaran Negara 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, (Lembaran Negara Tahun 2019 Nomor 222, Tambahan Lembaran Negara Nomor 6420).

Dewan Uni Eropa dan Parlemen Eropa, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (OJ L 119, Brussel, Belgia, 4 Mei 2016), 13, eur-lex.europa.eu.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan, (Lembaran Negara Tahun 2013 Nomor 232, Tambahan Lembaran Negara Nomor 5475).

Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas, (Lembaran Negara Tahun 2007 Nomor 106, Tambahan Lembaran Negara Nomor 4756).

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, (Lembaran Negara Tahun 2018 Nomor 182).