SNLPR: Siber Nusantara of Law and Politic Review
E-ISSN : 3089-2287
+62 822 1012 3600 https://research.e-siber.org/SNLPR siberpublisher.info@gmail.com
DOI: https://doi.org/10.38035/v3i1
https://creativecommons.org/licenses/by/4.0/
Received: 08 November 2026 | **Revised:** 10 November 2026 | **Accepted:** 11 November 2026

A Juridical Review of the Formulation of a Data Sharing Agreement in the Digital Service Ecosystem of the Indonesian National Police Based on the Personal Data Protection Law

Enjang Priambodo[1], Edi Saputra Hasibuan[2], Diana Fitriana[3]
[1]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, 202620261071@mhs.ubharajaya.ac.id
[2]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, edi.saputra@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, diana.fitriana@dsn.ubharajaya.ac.id

Corresponding Author: 202620261071@mhs.ubharajaya.ac.id[1]

Abstract: The acceleration of digital transformation toward realizing Police 4.0 requires the Indonesian National Police (Polri) to integrate public services and engage in massive data sharing with third parties, including government ministries/agencies and private partners. However, this system interconnectivity triggers cyber risks and serious threats of personal data breaches, as confirmed by various nationwide data breach incidents. Unlike prior studies that generally focus on general compliance review of the Personal Data Protection Law (UU PDP) or macro-level government data governance, this research specifically fills a research gap concerning the contractual instruments governing the legal relationship between Polri and third parties in technology-based public data sharing. This research analyzes the legal gap resulting from the absence of internal technical regulations adopting the Data Protection by Design principle in the development of police service applications, as well as the inadequacy of conventional Cooperation Agreements (Perjanjian Kerja Sama/PKS) and Non-Disclosure Agreements (NDA). Based on interviews with three vendors and an analysis of the contract documents they provided, these existing instruments are limited to confidentiality provisions and fail to accommodate compliance clauses in accordance with Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), such as purpose limitation, mandatory notification of personal data protection failures, cyber compliance audit rights, and indemnification clauses. This research aims to address two main issues: first, how aligned the application development and data exchange mechanisms in Polri's digital service ecosystem are with the UU PDP, and what this implies for the allocation of legal liability between Polri as the Personal Data Controller and private vendors as Personal Data Processors within the police data-sharing scheme; and second, how an ideal Data Sharing Agreement (DSA) clause formulation should be structured to ensure compliance with the UU PDP. Employing a normative juridical research method through statutory and conceptual approaches, both issues are analyzed comprehensively. The results of this research formulate a standardized and binding Data Sharing Agreement (DSA) to ensure legal certainty, mitigate legal liability and reputational risks for Polri as an institution, and provide optimal protection of the privacy rights of the public as data subjects.

Keywords: Data Sharing Agreement, Polri Digital Services, Personal Data Protection, Police 4.0, Personal Data Protection Law.

INTRODUCTION

Advances in information technology and the acceleration of national digital transformation through the Electronic-Based Government System (*Sistem Pemerintahan Berbasis Elektronik*/SPBE), as regulated in Presidential Regulation Number 95 of 2018, require every government agency to achieve integrated public services. In response, the Indonesian National Police (Polri) has adopted the *Police 4.0* paradigm, which rests on digitalization and real-time system interoperability. Digital service ecosystems such as *Electronic Traffic Law Enforcement* (ETLE), SIM *Online*, SKCK *Online*, and SuperApp Polri require massive data sharing with various third parties, including ministries/agencies and private technology service providers. This cooperation through *Application Programming Interfaces* (APIs) is in line with Presidential Regulation Number 82 of 2023 on the Acceleration of Digital Transformation and the Integration of National Digital Services, which promotes the massive integration and interoperability of SPBE applications to improve accessibility and the efficiency of public services, but it has not been matched by legal instruments that adequately regulate the allocation of responsibility for data. Presidential Regulation Number 39 of 2019 on One Data Indonesia likewise regulates data produced by agencies in support of development and contains no provisions on personal data.

The interconnection of systems and the large-scale flow of data give rise to significant cyber vulnerabilities, particularly with regard to the protection of the public's personal data. A series of nationwide data breach incidents involving public agencies underscores this, among them the exposure of billions of SIM card registration records in 2022 (CNN Indonesia, 2022), the leak of BPJS Kesehatan patient data in 2021 (Kompas, 2021), and the vulnerability of the Ministry of Health's e-HAC application caused by a third party's server misconfiguration (Reuters, 2021). These three precedents show that infrastructure or systems integrated with private vendors often become the main security gap, and they underscore the high legal risk faced by public institutions in the absence of binding instruments that clearly regulate the *boundary of liability* with service-provider partners.

The enactment of Law Number 27 of 2022 on Personal Data Protection (UU PDP) has brought a paradigm shift in data governance in Indonesia. The law requires the security and supervision of data processing (Articles 35, 37, and 39), which serve as the basis for interpreting the *Data Protection by Design* principle, and it establishes the allocation of responsibility between the Personal Data Controller (*Data Controller*) and the Personal Data Processor (*Data Processor*) under Articles 51 and 52 of the UU PDP. In its service ecosystem, Polri acts as the Data Controller, while private partners act as Data Processors. In practice, application development within Polri is still predominantly focused on user-interface functionality and ease of transactions, and has not yet fully integrated privacy compliance standards from the earliest stage of system architecture.

This condition results in a technical legal gap in operational cooperation instruments. The involvement of third parties is generally still based on conventional cooperation agreements (*Perjanjian Kerja Sama*/PKS) and general confidentiality clauses or *Non-Disclosure Agreements* (NDA) that focus more on the confidentiality of institutional information. These existing instruments are inadequate because they fail to accommodate crucial clauses mandated by the UU PDP, such as *purpose limitation*, the obligation to notify personal data protection failures within a set time limit (Article 46), cyber compliance *audit rights*, and *indemnification* clauses/mechanisms. The absence of a standard draft *Data Sharing Agreement* (DSA) places Polri at high liability risk if a system failure occurs on the third party's side. The formulation of a DSA based on the UU PDP is therefore indispensable to ensure legal certainty, mitigate institutional risk, and protect the privacy rights of data subjects. This research is limited to the relationship between Polri as the Personal Data

Controller and technology service-provider vendors as Personal Data Processors, with data subjects comprising members of the public and Polri members.

Based on the foregoing, this article examines two issues. First, how aligned the application development and data exchange mechanisms in Polri's digital service ecosystem are with the UU PDP, and what this implies for the allocation of legal liability between Polri as the Personal Data Controller and the third party as the Personal Data Processor when a personal data protection failure occurs. Second, how the main clauses of an ideal and binding *Data Sharing Agreement* (DSA) should be formulated to ensure legal certainty and the protection of personal data in Polri's digital service cooperation.

METHOD

This research uses normative legal research (*doctrinal legal research*), which focuses on the inventory of positive law, the discovery of legal principles, and the synchronization of statutory regulations on the governance and protection of personal data. To examine the legal issues comprehensively, the research combines two approaches: the statute approach and the conceptual approach. The statute approach is carried out by examining Law Number 27 of 2022 on Personal Data Protection (UU PDP); Presidential Regulations Number 95 of 2018, Number 39 of 2019, and Number 82 of 2023; Law Number 1 of 2024 on the second amendment to the Law on Electronic Information and Transactions; and Regulation of the Indonesian National Police (Perpolri) Number 4 of 2022 on One Data of the Indonesian National Police. The conceptual approach, grounded in the Theory of Legal Certainty (Radbruch, Fuller, and Otto) and the Theory of Legal Liability (Kelsen), is used to build legal arguments on the *Data Protection by Design* principle and the limits of legal liability. Articles 25 and 28 of the *General Data Protection Regulation* (GDPR) are referred to only as a comparison, not as a separate approach.

Legal materials were collected through library research, with the stages of inventory, categorization, and systematization of documents related to the research object. These include statutory regulations as primary legal materials, as well as practice data in the form of direct interviews with three vendors that develop Polri service applications, supported by contract documents provided by the interviewees; the identities of the interviewees and applications are anonymized. All collected materials were then analyzed qualitatively and prescriptively using deductive reasoning. The analysis starts from a major premise consisting of the normative and compliance provisions of the UU PDP, which is then applied to a minor premise consisting of findings from the interviews and the analysis of contract documents on gaps in the drafting of ICT cooperation agreements within Polri. The results of the analysis are directed toward a concrete prescription in the form of a comprehensive and binding standard *Data Sharing Agreement* (DSA) clause formulation. Two of the applications built by the vendors process different categories of data, namely data on Polri members and data on members of the public at the time of application registration, so the findings cover two groups of data subjects. Given the limited number of interviewees, the findings are understood as a description of practice, not as a generalization for all Polri vendors.

RESULTS AND DISCUSSION

Alignment of Polri's Application Development and Data Exchange Mechanisms with the UU PDP.

The transformation of police services toward the *Police 4.0* paradigm has triggered large-scale system interconnection between Polri and third parties. However, this acceleration of operational interoperability has not run in line with legal compliance on personal data protection. The UU PDP does not formulate the *Data Protection by Design* principle explicitly. The closest bases are Article 35 of the UU PDP, which requires the Controller to prepare and implement operational technical measures and to determine the level of security

according to the nature and risk of the data, and Article 39, which requires the prevention of unauthorized access through a reliable, secure, and accountable security system. Both provisions also apply to the Processor (Article 52) and are in line with Article 15 of the Electronic Information and Transactions (ITE) Law as amended by Law Number 1 of 2024. Article 25 of the GDPR, which formulates "*data protection by design and by default*," serves as a comparison. In this article, the principle is understood as a systematic interpretation that personal data protection must be designed from the earliest stage of application development.

Data exchange regulations likewise do not yet contain provisions on personal data protection. Perpolri Number 4 of 2022 regulates data exchange with ministries/agencies and other parties through API-based cooperation carried out centrally through the *Walidata* (data custodian) (Article 9), and the *Walidata* is tasked with ensuring the security of data and information. However, that regulation does not contain personal data protection provisions as regulated in the UU PDP.

The facts on the ground show a significant disparity with the mandate of the law. The application development process within Polri is currently still predominantly oriented toward user-interface functionality and transaction efficiency, without integrating privacy compliance audit instruments. This gap is evident from interviews with three vendors and an analysis of the contract documents provided by the interviewees. Two of the applications process different personal data: one application manages data on Polri members, while the other manages data on members of the public at registration, including the National Identity Number (NIK). In the case of both vendors, the contract was not accompanied by a separate *Non-Disclosure Agreement* (NDA) document. Confidentiality is regulated only as a general clause within the contract, which protects the contract documents, technical specifications, and project information. One other vendor had an NDA for the development of an older application, but its content was limited to data confidentiality and must be read in the context of when it was made. The contracts reviewed contain a risk indemnification clause, but its scope is limited to physical loss and property damage and ends upon handover, and it does not cover personal data protection failures. These documents have not elaborated the obligations of the UU PDP in the form of clauses, including purpose limitation (Article 28), supervision of parties involved in processing (Article 37), deletion or destruction of data (Article 44), notification of personal data protection failures (Article 46), and written approval for sub-processors (Article 51 paragraphs (4) and (5)). In addition, there is not yet a standard for drafting NDA or *Data Sharing Agreement* (DSA) clauses.

The absence of a separate NDA at two vendors, and the limited scope of the NDA at the other vendor, which regulates only confidentiality, show that the personal data protection obligations under the UU PDP have not yet been bound contractually. Without a contractual commitment requiring security standards from the procurement phase, vendors work without a clear legal corridor for privacy protection. This practice makes the security architecture protecting the public's data depend purely on the good faith and internal policies of vendors, rather than on legal compliance standards that can be demanded or audited juridically. This shows that Polri's digital service ecosystem has not yet fully made data protection a binding operational and administrative prerequisite.

Allocation of Roles and Limits of Legal Liability (*Legal Liability*).

The UU PDP restructures the governance of data-exchange cooperation by classifying legal subjects into two main roles: the Personal Data Controller (*Data Controller*) and the Personal Data Processor (*Data Processor*). Polri is institutionally the Personal Data Controller because it determines the purposes and exercises control over processing (Article 1 point 4 of the UU PDP), while the ICT Division (Div TIK), as *Walidata*, and the application-owner work units are understood as internal units that carry out this control function. The roles of Data Steering Body (*Pengarah Data*), *Walidata*, and Data Producer (*Produsen Data*)

in Perpolri Number 4 of 2022 are One Data governance roles, not roles under the UU PDP. By contrast, private vendors or cloud-infrastructure providers engaged by Polri act as Data Processors. Article 51 paragraph (3) of the UU PDP stipulates that processing by a Processor falls within the Controller's responsibility, unless the Processor processes outside the Controller's instructions and purposes (Article 51 paragraph (6)), while Article 52 binds the Processor to security and supervision obligations. The Controller's burden of responsibility is therefore greater, covering the fulfillment of data subject rights through to the notification of personal data protection failures (Article 46). It should be noted that Article 50 of the UU PDP exempts some of the Controller's obligations for the purposes of law enforcement proceedings, so the risk discussed in this article must be distinguished from Polri's law enforcement function. The processing of Polri members' personnel data and of public service registration data is not automatically part of law enforcement proceedings.

The absence of a specific legally binding instrument regulating privacy management between the two entities creates a blurred boundary of responsibility (*legal gap*) that gives rise to asymmetric liability risk. Under the civil law doctrine of the standard of care (*duty of care*), negligence in supervision can have grave consequences for a public institution. Where a personal data protection failure (*data breach*) arises from a vulnerability in a vendor's server or system, Polri remains at high risk of being the first party sued in civil proceedings or subjected to administrative sanctions (a damages claim by the data subject under Article 12 paragraph (1), an assessment of negligence in supervising parties involved in processing under Article 37, and administrative sanctions under Article 57 of the UU PDP). Without a contract that details the limits of the vendor's responsibility, Polri's ability to claim back (right of recourse) from the third party becomes uncertain, although claims may generally be based on breach of contract (Article 1243 of the Indonesian Civil Code, KUHPerdata) or unlawful acts (Article 1365 of the Civil Code). Within the framework of the Theory of Legal Liability, responsibility needs to be distinguished into two layers. The first layer is responsibility to external parties, namely data subjects and the regulator, which remains with the Controller under Article 51 paragraph (3) of the UU PDP. The second layer is responsibility between the parties to the agreement, in the form of risk allocation, indemnification, and the right of recourse, which may be regulated through DSA clauses with due regard to the principles of freedom of contract and good faith (Article 1338 of the Civil Code).

Formulation of the Main Clauses of a *Standardized Data Sharing Agreement* (DSA).

In response to the inadequacy of cooperation agreements and the limited scope of NDAs in existing IT procurement cooperation, Polri urgently needs a standard *Data Sharing Agreement* (DSA) clause formulation as a derivative or mandatory annex to all contracts involving data exchange. In this article, a DSA is understood as a written agreement that serves as an annex or companion to the main cooperation agreement and regulates the conditions for processing Personal Data between Polri as the Controller and the third party as the Processor. Unlike an NDA, which focuses on confidentiality, a DSA elaborates the full range of personal data protection obligations, including accountability when a protection failure occurs. To ensure legal certainty grounded in the UU PDP, the Polri DSA formulation must include six material clauses that are comprehensive and reciprocally binding, namely:

1. First, the Purpose Limitation clause (*Purpose Limitation*). Article 28 of the UU PDP requires the Controller to process personal data in accordance with its purpose, and Article 51 paragraph (1) requires the Processor to process on the Controller's instructions. This clause extends that obligation to the vendor by prohibiting the vendor from using personal data for third-party analytics, monetization, or *cross-profiling* without Polri's written consent, so that data is not misused beyond the purpose of the cooperation.

2. Second, the Notification of Personal Data Protection Failure clause (*Data Breach Notification*). Article 46 paragraph (1) of the UU PDP requires the Controller to notify the Personal Data Subject and the institution in writing of a personal data protection failure no later than 3x24 hours. The Controller can fulfill this obligation only if the Processor first reports the incident to it. The DSA therefore needs to require the Processor to report any access anomaly or security incident to Polri within a shorter period than the 3x24-hour limit. This research proposes a maximum of 1x24 hours, so that Polri still has sufficient time to assess the incident and give notification in accordance with the provisions.
3. Third, the Compliance Audit Rights clause (*Audit and Inspection Rights*). Article 37 of the UU PDP requires the Controller to supervise every party involved in processing. This clause serves as the means of that supervision: Polri has the right to evaluate security periodically and to conduct *penetration testing* of the vendor's infrastructure, including when there are indications of an incident, to ensure that the security standards agreed in the *Service Level Agreement* (SLA) are met.
4. Fourth, the Data Retention and Destruction clause (*Data Retention and Destruction*). Articles 43 and 44 of the UU PDP require the Controller to delete and destroy personal data, among other things when the data is no longer needed or its retention period has expired. This clause passes that obligation on to the vendor: the vendor submits a Data Destruction Report (*Berita Acara Pemusnahan Data*) immediately after the contract period ends, and is prohibited from keeping *shadow backups* of Polri's databases or source code.
5. Fifth, the Sub-Processor clause. Article 51 paragraphs (4) and (5) of the UU PDP require the Controller's written approval if the Processor engages another processor. This clause prohibits the vendor from using sub-processors without Polri's written approval and requires the vendor to bind sub-processors to the same data protection obligations.
6. Sixth, the Indemnification and Right of Recourse clause (*Indemnification Clause*). Article 51 paragraph (3) of the UU PDP stipulates that processing by a Processor is the Controller's responsibility, so Polri remains responsible to data subjects and the regulator. This clause does not remove that responsibility, but gives Polri a contractual basis to claim back from the vendor, in proportion to the vendor's share of responsibility, losses arising from a security failure in the vendor's system or from processing outside the instructions and purposes set by Polri (Article 51 paragraph (6)).

Table 1. Matrix of Juridical Analysis and *Data Sharing Agreement* (DSA) Formulation for Polri Digital Services

STUDY FOCUS	FACTUAL CONDITIONS / EMPIRICAL FINDINGS (*DAS SEIN*)	JURIDICAL REVIEW BASED ON THE UU PDP	LEGAL IMPLICATIONS AND SOLUTIONS
Alignment of Application Development with the Principles of the UU PDP	The design process focuses on the user interface (UI/UX). Interviews with three vendors and an analysis of the contract documents show that two vendors have no separate NDA (confidentiality is only a general clause in the contract),	Articles 35 and 39 of the UU PDP (and Article 15 of the ITE Law) require security commensurate with risk and a reliable security system; they are interpreted as the basis of the *Data Protection by Design* principle (comparison: Article 25 of the GDPR) and are not yet	System security currently depends on the vendor's good faith (*gentlemen's agreement*). Privacy protection must become a standard prerequisite in Polri's ICT procurement administration.

	while one vendor used an NDA for an older application, with content limited to data confidentiality.	reflected in application design.	
Position of Legal Subjects and Allocation of Responsibility (*Legal Liability*)	Absence of technical regulations and contract instruments that detail the limits of supervisory responsibility and of system failure between Polri and private partners.	Polri is institutionally the Data Controller, while the vendor is the Processor. Processing by the Processor is the Controller's responsibility (Article 51 paragraph (3)), unless the Processor acts outside the Controller's instructions and purposes (paragraph (6)).	Liability asymmetry arises (*duty of care*). If a vendor's system suffers a personal data protection failure, Polri risks being sued (Article 12) or subjected to administrative sanctions (Article 57), while its ability to claim back from the vendor (right of recourse) is uncertain.
Inadequacy of Existing Legal Instruments (PKS and NDA)	The conventional PKS and NDA instruments in use focus only on protecting the confidentiality of internal/institutional information, not the personal data of Polri members or the public.	The UU PDP requires operational compliance standards, namely purpose limitation (Article 28), supervision of involved parties (Article 37), data destruction (Article 44), notification of personal data protection failures (Article 46), and written approval of sub-processors (Article 51), which are not accommodated in ordinary PKS/NDAs.	A dedicated instrument is needed that focuses on the governance of the processing of Polri members' and the public's personal data by third parties, together with standards for drafting NDA and DSA clauses.
Formulation of Standard *Data Sharing Agreement* (DSA) Clauses	A vacuum of derivative legal instruments that can bindingly mitigate Polri's losses in procurement cooperation or in building ICT instruments.	The obligations of the Controller and Processor (Articles 28, 37, 44, 46, 51, and 52) need to be bound contractually through a *Standardized DSA*.	Formulation of 6 Mandatory DSA Clauses: 1. *Purpose Limitation* 2. *Data Breach Notification* (Max. 1x24 Hours) 3. *Audit & Inspection Rights* 4. *Data Retention & Destruction* 5. *Sub-processor & Oversight* (Sub-Processor Approval). 6. *Indemnification* and Right of Recourse.

CONCLUSION AND RECOMMENDATIONS

Conclusion

The acceleration of Polri's digital transformation toward the *Police 4.0* ecosystem, which demands large-scale system interconnection with third parties, is not yet fully aligned with the mandate of Law Number 27 of 2022 on Personal Data Protection (UU PDP). The practice of procuring and building technology-based services within Polri is still

predominantly oriented toward functionality and has not made the *Data Protection by Design* principle a built-in prerequisite in system architecture. Interviews and an analysis of contract documents at three vendors show this operational legal vacuum: conventional contracts without a separate NDA at two vendors, and an NDA limited to confidentiality at the other vendor, so that the obligations of the UU PDP have not been elaborated. The inadequacy of these existing legal instruments gives rise to an asymmetry of responsibility that is highly detrimental to the institution. The absence of clear limits of liability could leave Polri as Data Controller bearing a disproportionate burden of supervisory negligence, and at high risk of facing a series of civil claims and administrative sanctions if a security failure occurs in the infrastructure of a private partner acting as Data Processor. A DSA is therefore needed that contains six main clauses, namely purpose limitation, notification of personal data protection failures, audit rights, data destruction, sub-processors, and indemnification and the right of recourse, which transfers part of the financial burden to the Processor without removing Polri's responsibility as Controller to data subjects and the regulator.

Research Limitations

This research is limited to the relationship between Polri as the Personal Data Controller and technology service-provider vendors as Personal Data Processors, with data subjects comprising members of the public and Polri members. The legal liability examined is contractual, civil, and administrative in nature; criminal liability under the UU PDP is outside its scope. The practice data come from interviews with three vendors, supported by the contract documents they provided, so the findings describe practice in that sample and cannot be generalized to all Polri vendors. The DSA clause formulation, including the proposed 1x24-hour notification period, is a prescriptive recommendation that has not yet been tested in contractual practice.

Recommendations

As a constructive step to minimize liability risk and maintain institutional credibility, Polri is advised to prepare internal technical guidelines that integrate a *Standardized Data Sharing Agreement* (DSA) into every procurement and IT service development process. This DSA formulation is expected to serve as a complementary protective instrument that always accompanies the main cooperation contract, containing essential clauses that bridge compliance with the UU PDP. The clauses should cover purpose limitation for data processing, a mechanism for the vendor to report security incidents within an adequate time limit, Polri's authority to evaluate cyber compliance, procedures for destroying data after the contract ends, written approval for the involvement of sub-processors, and an agreement on a proportionate allocation of responsibility (*indemnification*). In addition, internal Polri stakeholders, particularly the ICT Division and the Polri Legal Division, are advised to begin adopting the *Data Protection by Design* principle as an operational standard from the earliest stage of application design. This proactive approach aims to ensure that the governance of the public's personal data protection no longer depends merely on vendors' internal policies, but runs in a structured manner and has binding legal certainty for the entire ecosystem of service-provider partners.

REFERENCES

Cavoukian, Ann. (2009). Privacy by Design: The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario.

Fuller, Lon L. (1969). The Morality of Law. New Haven: Yale University Press.

Kelsen, Hans. (2006). Teori Umum tentang Hukum dan Negara [General Theory of Law and State], translated by Raisul Muttaqien. Bandung: Nusa Media.

Marzuki, Peter Mahmud. (2011). Penelitian Hukum [Legal Research]: Revised Edition. Jakarta: Kencana Prenada Media Group.

Makarim, Edmon. (2010). Tanggung Jawab Hukum Penyelenggara Sistem Elektronik [Legal Liability of Electronic System Operators]. Jakarta: Rajawali Pers.

Mertokusumo, Sudikno. (2007). Mengenal Hukum: Suatu Pengantar [Getting to Know Law: An Introduction]. Yogyakarta: Liberty.

Otto, Jan Michiel. (2006). Kepastian Hukum di Negara Berkembang [Legal Certainty in Developing Countries]. Jakarta: Proyek Pembinaan Badan Pembinaan Hukum Nasional.

Rosadi, Sinta Dewi. (2015). Hukum Privasi dan Pelindungan Data Pribadi di Indonesia [Privacy Law and Personal Data Protection in Indonesia]. Bandung: PT Citra Aditya Bakti.

Abdurrahman, A., & Herawati. (2023). "Urgensi Pelindungan Data Pribadi dalam Implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE)" [The Urgency of Personal Data Protection in the Implementation of the Electronic-Based Government System (SPBE)]. Jurnal Hukum Tata Negara, 10(2), 145-160.

Pramono, B., & Setiawan, R. (2022). "Tanggung Jawab Hukum Pihak Ketiga atas Kebocoran Data dalam Perjanjian Cloud Computing" [Legal Liability of Third Parties for Data Breaches in Cloud Computing Agreements]. Jurnal Hukum Siber dan Teknologi, 5(1), 33-48.

Yuniarti, S. (2020). "Pembatasan Pertanggungjawaban (Limitation of Liability) dalam Kontrak Elektronik B2B" [Limitation of Liability in B2B Electronic Contracts]. Jurnal Hukum Bisnis Digital, 3(2), 77-92.

Law Number 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette Number 6820).

Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette Number 6905).

Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata/Burgerlijk Wetboek).

Presidential Regulation Number 95 of 2018 on the Electronic-Based Government System (State Gazette of the Republic of Indonesia of 2018 Number 182).

Presidential Regulation Number 39 of 2019 on One Data Indonesia (State Gazette of the Republic of Indonesia of 2019 Number 112).

Presidential Regulation Number 82 of 2023 on the Acceleration of Digital Transformation and the Integration of National Digital Services (State Gazette of the Republic of Indonesia of 2023 Number 159).

Regulation of the Indonesian National Police Number 4 of 2022 on One Data of the Indonesian National Police (State Bulletin/Berita Negara of the Republic of Indonesia of 2022 Number 310).

General Data Protection Regulation (GDPR) – 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.

Badan Siber dan Sandi Negara (BSSN) [National Cyber and Crypto Agency]. (2022). Laporan Tahunan Monitoring Keamanan Siber 2022 [2022 Annual Cybersecurity Monitoring Report]. Jakarta: Direktorat Operasi Keamanan Siber BSSN.

CNN Indonesia. (2022). "Dugaan 1,3 Miliar Data SIM Card Bocor dan Saling Lempar Tanggung Jawab" [Alleged Leak of 1.3 Billion SIM Card Records and Mutual Blame Over Responsibility], accessed from https://www.cnnindonesia.com/teknologi/20220909190301-192-845818/kasus-kebocoran-13-miliar-data-di-ri-disebut-terbesar-di-asia on 26 September 2026.

Kompas. (2021). "Kasus Kebocoran Data 279 Juta Penduduk di BPJS Kesehatan" [The Case of the Leak of 279 Million Residents' Data at BPJS Kesehatan], accessed from https://www.kompas.com/tren/read/2021/05/21/201500565/bahaya-kebocoran-data-yang-diduga-dari-laman-bpjs-ini-kata-ahli-it?page=all on 26 September 2026.

Reuters. (2021). "Vulnerability in Indonesia's e-HAC Application Exposes Personal Data of Millions," accessed from https://www.thejakartapost.com/news/2021/08/31/authorities-probe-suspected-ehac-data-breach-of-1-million-users on 26 September 2026.

Interviews with Interviewees from Vendor A, Vendor B, and Vendor C (providers of Polri service application development services; identities anonymized), conducted on 26 September and 15 October 2026.