JURNAL LITIGASI

Available online at: *journal.unpas.ac.id/index.php/litigasi*

Jurnal LITIGASI, Vol. 27 (2) October, 2026, p. 104-137
doi.org/10.23969/litigasi.v27i2.63990

Reconstructing Personal Data Protection in Indonesia's Digital Transportation Sector: Liability, Contractual Justice, and Cybersecurity

Siti Mariyam[(1)]
Faculty of Law, Universitas 17 Agustus 1945 (UNTAG) Semarang, Indonesia
Email: sitimariyam@untagsmg.ac.id

Ceprudin[(2)]
Faculty of Law, Universitas 17 Agustus 1945 (UNTAG) Semarang, Indonesia
Email: Ceprudin@untagsmg.ac.id

Hillan Syamsudhuha Ahmad el Hariz[(3)]
Faculty of Computer Science, Universitas Amikom Purwokerto, Indonesia
Email: samhillan50@gmail.com

Georges Olemanu Lohalo[(4)]
Université de Kinshasa, and Centre de recherche en sciences humaines -CRESH, Democratic Republic of the Congo
Email: georgeslohalo@gmail.com

ABSTRACT

Indonesia's digital transportation sector faces a tension between mobility efficiency and the vulnerability of users' personal data, as application providers characterise themselves as technology platforms while standard electronic contracts may allocate the risk of data breaches to consumers and driver-partners. This study examines how Minister of Transportation Regulation Number 118 of 2018 and Law Number 27 of 2022 concerning Personal Data Protection should be synchronised in determining the responsibility of application providers, to what extent exoneration clauses are compatible with contractual justice and data protection law, and what regulatory architecture should integrate cybersecurity into digital transportation governance. Using normative legal research with statutory and conceptual approaches, the study analyses legislation, literature, and the standard terms and privacy policies of dominant application providers through operational indicators of legal certainty and of commutative, distributive, and procedural justice. The findings demonstrate that regulatory synchronisation strengthens the normative basis for enhanced liability of application providers for personal data breaches, including a reversed burden of proof in consumer claims, and supports a stricter liability regime for high-risk processing as a proposal for future legislation. Exoneration clauses that transfer the provider's liability are void by operation of law without invalidating the whole contract, while personal data may constitute additional economic consideration where their processing exceeds what the transport service requires. The study proposes an Integrated Digital Transportation Data Governance Framework built on regulatory integration, platform accountability, contractual justice, and risk-based cybersecurity governance, including tiered certification, impact assessments, and coordinated supervision.

Keywords: *Personal Data Protection, Digital Transportation, Platform Liability, Exoneration Clauses, Cybersecurity*

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Available online at: *journal.unpas.ac.id/index.php/litigasi*
Jurnal LITIGASI, Vol. 27 (2) October, 2026, p. 104-137
doi.org/10.23969/litigasi.v27i2.63990

I. INTRODUCTION

The transportation sector occupies a strategic position in national economic development, consistent with the mandate in the fourth paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia. The fourth industrial revolution has integrated cyber-physical systems and the Internet of Things into service sectors, including transportation, giving rise to application-based transport services that have radically transformed urban mobility (Mariyam et al., 2026). Such digital transformation reshapes not only markets but also the institutions through which legal relationships are formed and legal authority is exercised, while generating new areas of legal ambiguity (Anggono et al., 2025).

These services, however, require users to provide personal data, including names, phone numbers, precise addresses, geolocation, and financial information. Article 28G paragraph (1) of the 1945 Constitution guarantees every person the protection of their person, family, honour, dignity, and property under their control, affirming the state's obligation to protect citizens' personal data in the digital sphere, including in commercial electronic transactions (Mariyam, 2019b). Such constitutional guarantees become effective only when translated into clear regulation and accessible procedures.

Minister of Transportation Regulation Number 118 of 2018 concerning the Operation of Special Rental Transport defines special rental transport as a door-to-door service booked through a technology-based application and treats Application Companies and Special Rental Transport Companies as distinct legal subjects. Article 12 governs the business form of Special Rental Transport Companies, whereas Article 31 requires both types of company to apply fair and transparent treatment and to guarantee the confidentiality and security of service users' data (Mariyam, 2019a).

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

The legal relationship among application providers, driver-partners, and consumers is formed through electronic contracts, which Law Number 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law Number 1 of 2024, recognises as binding where they satisfy the requirements of Article 1320 of the Indonesian Civil Code. The efficiency of electronic contracting carries inherent risks, such as personal data breaches, electronic system hacking, and digital identity fraud (Sanjaya et al., 2026).

Law Number 27 of 2022 concerning Personal Data Protection, fully applicable since October 2024, consolidates previously scattered rules and imposes security obligations on personal data controllers. Transportation application providers will, in most of their processing operations, qualify as controllers because they determine the purposes of processing and exercise control over it, and therefore bear responsibility throughout the data life cycle. The obligation to protect user data in this ecosystem thus rests on transportation law, electronic transactions law, and personal data protection law, with privacy by design as one technical manifestation that ought to be inherent in every mobile application architecture (Rejeki, 2026).

Public acceptance is widespread: consumers choose online transportation mainly for affordable fares (84.1%), faster travel (81.9%), fleet comfort (78.8%), and safety (61.4%) (Novalius, 2017). Although these figures are dated, the structural drivers of demand they reflect continue to sustain a growing aggregation of personal data on providers' servers.

This digitalisation is matched by rising cybersecurity threats. The Microsoft Digital Defence Report 2024 ranks transportation as the fifth most targeted sector worldwide, accounting for 5% of detected incidents (Microsoft, 2024), a consequence of infrastructure that is connected to global networks and processes real-time transactions at scale (Olasehinde et al., 2026). The absence

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

of an Information Security Management System, such as one based on ISO/IEC 27001, increases the risk of operational disruption, reputational harm, and infringement of the right to personal data protection (Findrikova & Kubina, 2026).

Despite this normative framework, four legal issues can be identified. The first concerns the characterisation of application providers as technology platforms rather than public transportation companies, which underpins the classification of drivers as partners and is invoked to limit providers' responsibility for acts committed by driver-partners in the field (Sepriadi et al., 2026).

The second concerns contractual fairness. Standardised, unilaterally drafted terms may disclaim responsibility for third-party actions or require users to waive compensation claims for data misuse, raising questions of good faith and of the protection of the structurally weaker party (Desril & Santoso, 2026). The formal validity of electronic contracts may thus be used to legitimise a disproportionate transfer of liability (Sari et al., 2026).

The third concerns operational vulnerability. Driver-partners may access users' home geolocation, workplace location, and phone numbers, creating a risk of use beyond the transport service, while they themselves are exposed to fraud such as fake orders (Satria, 2025). A regulatory focus limited to consumers also overlooks driver-partners, who provide identity documents, licensing documents, and biometric data to application providers.

The fourth concerns the lack of synchronisation between Minister of Transportation Regulation Number 118 of 2018 and internationally recognised cybersecurity standards. Article 31 does not specify the technical standards required, although secure digital transactions demand confidentiality, integrity, availability, and non-repudiation (Wijaya et al., 2025), and therefore

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

leaves the level of information security largely to each provider's discretion (I. Made et al., 2025).

This normative gap matters on two theoretical grounds. Legal certainty demands clarity of norms, consistency among regulations, predictability of consequences, and enforceability, yet uncertainty over regulators' jurisdiction and the liability applicable to data breaches weakens existing instruments (Agung & Nasution, 2023). Justice demands attention to the weaker contracting party, and liability-shifting clauses may undermine commutative justice where platforms derive value from data while declining responsibility for its security (Mashchenko & Radiev, 2023).

Prior research has examined these issues separately. Siti Mariyam et al. analyse exoneration clauses from the perspective of the Personal Data Protection Law and consumer law without confronting technical transportation regulation (Mariyam et al., 2026). Raja Desril and Mulia Akbar Santoso examine the partnership relationship without addressing personal data protection (Desril & Santoso, 2026). Opik Sepriadi et al. concentrate on the validity of electronic contracts (Sepriadi et al., 2026), while Dominika Findriková and Milan Kubina address ISO/IEC 27001 implementation from a managerial perspective without the Indonesian legal framework (Findrikova & Kubina, 2026).

Fikri and Rusdiana likewise observe that personal data protection in Indonesian positive law has been examined in general terms rather than within the transportation sector (Fikri & Rusdiana, 2023), even though the gap between formal recognition and operational safeguards recurs across domains, from genetic data used as evidence in family disputes (Abdillah et al., 2026) to beneficiary data in public welfare programmes. To address this gap, the study proposes an Integrated Digital Transportation Data Governance Framework

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

with four pillars: regulatory integration; platform accountability calibrated to control and processing risk; contractual justice through restrictions on exoneration clauses; and risk-based cybersecurity governance. Unlike prior studies, it confronts Minister of Transportation Regulation Number 118 of 2018 directly with Law Number 27 of 2022, evaluates contract terms through operational indicators of legal certainty and justice, and translates information security requirements into legislative and licensing proposals.

Accordingly, this study addresses three research questions: first, how Minister of Transportation Regulation Number 118 of 2018 and Law Number 27 of 2022 should be synchronised in determining the legal responsibility of application providers (Section III.A); second, to what extent exoneration clauses in digital transportation contracts are compatible with contractual justice and personal data protection law (Section III.B); and third, what regulatory architecture should integrate cybersecurity and personal data protection into Indonesia's digital transportation governance (Section III.C).

II. RESEARCH METHODS

This normative legal research (Audina Sukmawan et al., 2025) employs a statutory approach to examine the synchronisation of the Personal Data Protection Law, Minister of Transportation Regulation Number 118 of 2018, the Consumer Protection Law, and the Electronic Information and Transactions Law, and a conceptual approach to distinguish the models of liability, from fault-based liability and presumed fault to strict liability (Benuf & Azhar, 2020). Primary legal materials comprise these instruments together with the 1945 Constitution, the Civil Code, and Government Regulation Number 71 of 2019, supplemented comparatively by the General Data Protection Regulation, Directive (EU) 2019/770, and judgments of the Court of Justice of the European

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Union; secondary materials comprise books, journal articles, and policy documents.

Legal materials were collected through library research, including nine contractual documents from Gojek, Grab, and Maxim, the three providers that dominate the Indonesian ride-hailing market: for each provider, the consumer terms of service, the driver-partner terms, and the privacy policy in force on its official website when accessed in 2026. Clauses that limit liability, shift responsibility for data misuse, govern data processing, or restrict claims were evaluated against Article 18 of the Consumer Protection Law, Articles 1320, 1337, and 1349 of the Civil Code, and Articles 20, 34 to 39, 46, and 47 of the Personal Data Protection Law. These documents are treated as objects of legal evaluation, not as evidence of the providers' actual security practices.

The analysis proceeds through systematic interpretation, legal construction, and policy prescription, distinguishing existing law (*lex lata*) from the authors' proposals (*de lege ferenda*). Legal certainty and justice are operationalised through the indicators in Table 1: legal certainty through normative clarity, regulatory consistency, predictability, and enforceability (Firdaus, 2025); and justice through its commutative, distributive, and procedural dimensions (Aristotle, 2009).

Table 1. Analytical Indicators of Legal Certainty and Justice

Analytical lens	Indicator	Question applied to the legal materials
Legal certainty	Normative clarity	Do the norms identify the addressee, the required conduct, and the standard of compliance with sufficient precision?

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Analytical lens	Indicator	Question applied to the legal materials
Legal certainty	Regulatory consistency	Are PM 118/2018, the PDP Law, the Consumer Protection Law, and the EIT Law consistent in their terminology and in the obligations they allocate?
Legal certainty	Predictability of legal consequences	Can the parties foresee who bears liability, under which burden of proof, and with which defences, when a data breach occurs?
Legal certainty	Enforceability	Is there an identifiable institution, procedure, and sanction through which the norm can be enforced?
Commutative justice	Equivalence of performances and allocation of risk	Are rights, obligations, and risks between provider and user allocated in proportion to each party's performance, benefit, and control?
Distributive justice	Distribution of benefits and burdens	How are the economic benefits of data processing and the burdens of cybersecurity risk distributed among providers, consumers, and driver-partners?
Procedural justice	Transparency and access to remedies	Are consent mechanisms, information, complaint procedures, and remedies accessible and intelligible to data subjects?

Source: Compiled by the authors, 2026

III. RESEARCH RESULTS AND ANALYSIS

A. Regulatory Synchronisation and the Liability of Application Providers for Data Breaches

Application providers commonly describe themselves as technology platform providers rather than public land transportation companies. This characterisation distances them from the obligations that bind public transportation companies, including passenger safety, and raises the question

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

of whether they bear vicarious liability for acts committed by driver-partners (J. Zhang, 2024).

Minister of Transportation Regulation Number 118 of 2018 distinguishes the Special Rental Transport Company, which operates the service, from the Application Company, which provides the application. Article 12 governs only the business form of the transport company, whereas Article 31 is expressly addressed to Application Companies as well. Application providers are therefore subject to sector-specific obligations as Application Companies, to obligations as electronic system operators under the Electronic Information and Transactions Law and Government Regulation Number 71 of 2019, and to obligations as personal data controllers under the Personal Data Protection Law. Their data protection obligations thus do not depend on whether they are transport operators, a question that turns on their operational control over the carriage service and lies beyond this study (Zhou, 2022).

Technological advancement challenges the foundations of modern law (Anwar et al., 2026). Carriage law makes the carrier responsible for the safety of what is carried, and in the digital era this extends to passengers' digital identity, since names, phone numbers, geolocated travel history, and payment information are aggregated on a large scale (W. Zhang & Zhong, 2022).

Article 31 of Minister of Transportation Regulation Number 118 of 2018 requires Application Companies and Special Rental Transport Companies to apply fair, transparent, and reliable treatment and to guarantee the confidentiality and security of Service Users' data. It is an early legal recognition of privacy rights in the sector, but it is declaratory and lacks operational elaboration. Measured against the indicator of normative clarity, it specifies no cybersecurity parameters, no data retention period, and no mechanism for restoring consumers' rights after a breach.

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

This limited elaboration creates uncertainty in attributing liability, particularly because Terms of Service may contain exoneration clauses that release the provider where consumer data is misused by third parties, including driver-partners. Where such a clause transfers the business actor's own liability, it falls within the prohibition in Article 18 paragraph (1) letter a of Law Number 8 of 1999 concerning Consumer Protection (N. Made et al., 2024), the consequences of which are examined in Section III.B.

Law Number 27 of 2022 remedies this weakness. Under Article 1 point 4, a Personal Data Controller determines the purpose of, and exercises control over, processing, a qualification providers satisfy in most operations. Controllers must secure data through technical and operational measures (Article 35), maintain confidentiality (Article 36), supervise every party processing under their control (Article 37), prevent unlawful processing and access (Articles 38 and 39), notify breaches within three times twenty-four hours (Article 46), and demonstrate accountability (Article 47) (Yuspin et al., 2024). Article 37 is particularly relevant, since driver-partners access passenger data within an environment the provider designs and controls.

Civil liability for data breaches generally rests on Article 1365 of the Indonesian Civil Code, supplemented by Article 1367, and requires proof of an unlawful act, fault, damage, and causation (Teichmann & Wittmann, 2023). Applied to digital breaches, this standard is problematic: consumers lack the information, technical capability, and control over computing infrastructure needed to show how a provider's security controls failed, a burden approaching what is commonly referred to as *probatio diabolica*.

Four frequently conflated models of liability must therefore be distinguished. Under fault-based liability, the claimant proves every element, including fault. Under presumed fault, fault is presumed once the claimant

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

establishes the other elements, subject to rebuttal, and the reversal of the burden of proof is the procedural mechanism through which this presumption operates. Under strict liability, fault is irrelevant, and the defendant escapes liability only on narrowly defined grounds, such as force majeure or the sole fault of the injured party (American Law Institute, 1977). Table 2 maps these models against the Indonesian legal materials.

Table 2. Models of Liability and Their Basis in Indonesian Law

Liability model	Allocation of the burden of proof	Basis in Indonesian law	Status in this study
Fault-based liability	Claimant proves the unlawful act, fault, damage, and causation	Articles 1365 and 1367 of the Civil Code	Existing positive law; default route for data subjects, including driver-partners
Presumed fault with reversed burden of proof	Defendant must prove absence of fault; claimant proves damage and causation	Articles 19 and 28 of the Consumer Protection Law (consumer claims); Article 15 of the EIT Law (operator responsibility subject to defences)	Existing positive law for consumer claims; basis for enhanced accountability
Accountability-based evidentiary presumption	Controller must demonstrate appropriate security measures once a breach within its system and resulting damage are shown	Articles 35–39 and 47 of the PDP Law, read systematically	Authors' proposed interpretation

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Liability model	Allocation of the burden of proof	Basis in Indonesian law	Status in this study
Strict liability	Liability without proof of fault; damage and causation still required; narrow defences (force majeure, sole fault of the data subject)	Not provided in the PDP Law; express legislative model in Article 88 of Law Number 32 of 2009	*De lege ferenda* proposal for clearly defined high-risk processing

Source: Compiled by the authors, 2026

As Table 2 indicates, the Personal Data Protection Law contains no provision eliminating the need to prove fault. Article 12 paragraph (1) grants data subjects the right to sue and receive compensation in accordance with laws and regulations, thereby referring back to general civil liability, while Article 47 establishes the principle of accountability. Accountability allocates the duty to demonstrate compliance, whereas strict liability determines responsibility for damage without proof of fault, so the two cannot be equated (Karjalainen, 2022). Where the Indonesian legislature intends liability without fault, it says so expressly, as in the absolute liability (*tanggung jawab mutlak*) provision of Article 88 of Law Number 32 of 2009 concerning Environmental Protection and Management.

The comparative framework shows the same distinction. The General Data Protection Regulation couples the accountability principle in Articles 5(2) and 24 with the security obligation in Article 32 and the right to compensation in Article 82 (Karjalainen, 2022). Article 82(3) exempts a controller that proves it is not in any way responsible for the event giving rise to the damage, and the Court of Justice of the European Union has held that an unauthorised disclosure is not in itself proof that the controller's measures were inappropriate, but that

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

the controller bears the burden of proving their appropriateness. The European regime is therefore one of presumed fault with a reversed burden of proof rather than pure strict liability (Lintvedt, 2022).

In Indonesian positive law, the strongest existing basis for enhanced liability lies in consumer protection law. Article 19 of the Consumer Protection Law obliges business actors to compensate consumers for damage resulting from their services, and Article 28 places on them the burden of proving the absence of fault, so a passenger's compensation claim against an application provider benefits from a reversed burden of proof. Article 15 of the Electronic Information and Transactions Law similarly makes electronic system operators responsible for the secure operation of their systems, subject to the defences of force majeure and user fault. These provisions support presumed fault, not strict liability. They also do not benefit driver-partners, who are not consumers in their partnership relationship and must rely on Article 1365 of the Civil Code and Article 12 of the Personal Data Protection Law.

Beyond these provisions, this study proposes that the accountability principle in Article 47, read with Articles 35 to 39 of the Personal Data Protection Law, justifies an evidentiary presumption. Once the data subject shows that a breach occurred within a system under the controller's control and that damage resulted, the controller should demonstrate that it implemented appropriate technical and operational measures, since it alone holds the relevant evidence and is already obliged to demonstrate compliance. This is a proposed interpretation informed by the reasoning in Case C-340/21, not an existing statutory rule; it does not dispense with causation and leaves room for the defences of force majeure and the data subject's own conduct.

Strict liability, by contrast, is more defensibly presented as a *de lege ferenda* proposal limited to clearly defined high-risk processing. The doctrine has

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

historically applied to abnormally dangerous activities, and certain processing in digital transportation shares their characteristics: continuous real-time geolocation tracking, large-scale processing of the data of millions of users, and the processing of biometric and financial data, which Article 34 paragraph (2) of the Personal Data Protection Law already treats as high-risk and whose breach may cause identity theft, financial loss, and threats to physical safety. A future amendment could impose liability without proof of fault for such processing, subject to proof of damage and causation and to narrow defences such as force majeure and the sole fault of the data subject (Teichmann & Wittmann, 2023).

Consider a driver-partner who retains a passenger's phone number and later uses it for harassment. Under the proposed approach, the question extends to whether the provider implemented measures under Articles 35 and 37 of the Personal Data Protection Law, such as role-based access control, number masking, and access that expires when the trip ends. The defence that the driver acted beyond company control is relevant but not decisive, while compliance by any particular provider remains an empirical question for technical audit.

Assessed against Table 1, the fragmentation between transportation and data protection regulation reduces normative clarity, consistency, and predictability (Firdaus, 2025), and an isolated reading of Minister of Transportation Regulation Number 118 of 2018 reduces providers' obligations to fares, roadworthiness, and licences, obligations that no longer reflect the risk profile of platform transport.

Read systematically with the Personal Data Protection Law, Article 31 acquires operational content and an enforcement mechanism. This reading narrows providers' reliance on their platform characterisation and strengthens

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

enhanced accountability, while strict liability remains a matter for future legislation.

Synchronised regulation does not, however, automatically invalidate every standard clause. The content, function, and effect of each clause must be assessed to determine whether it transfers the provider's liability in a prohibited manner, as examined in Section III.B. Synchronisation also requires the Ministry of Transportation, together with the personal data protection institution, to revise licensing procedures so that feasibility assessments cover periodic cybersecurity audits calibrated to risk, as discussed in Section III.C.

B. Personal Data as Hidden Consideration and the Validity of Exoneration Clauses in Digital Transportation

The electronic contract, frequently embodied in Terms of Service, is the principal instrument through which providers allocate litigation and damage risks, including through exoneration clauses that limit, transfer, or eliminate the drafter's liability (Bachelet, 2024).

Such clauses may state that the provider acts only as a technology intermediary and may require users to waive the provider's liability for incidents caused by third parties, including driver-partners. The analysis addresses their legal function rather than their precise wording, which differs among providers and changes with each update. Consent is typically given through a clickwrap mechanism, such as ticking an “I Agree” box, which is treated as binding but cannot displace the mandatory obligations that the Personal Data Protection Law imposes on data controllers (Guggenberger, 2025).

Formal validity under the Electronic Information and Transactions Law may thus legitimise attributing data breaches or geolocation misuse to drivers'

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

individual fault (Zhou, 2022), although allocating all risks of a data-driven business model to users is difficult to reconcile with commutative justice.

Freedom of contract assumes parties of equal standing and balanced negotiating capacity (Stewart & Williams, 2023), an assumption the platform economy challenges: consumers and driver-partners face a take-it-or-leave-it situation in which they must accept standardised terms in full or forgo the service or the platform as a source of income, while providers retain the power to amend their policies unilaterally (Guggenberger, 2025).

Consent obtained through the clickwrap instrument may therefore be formally valid while being substantively constrained by structural and economic necessity, reflecting a significant imbalance in bargaining power (Bachelet, 2024).

It is therefore important to distinguish the legal bases on which personal data are processed. Article 20 paragraph (2) of the Personal Data Protection Law recognises explicit consent, contract performance, legal obligation, vital interests, public interest, and legitimate interests. Data strictly necessary for the trip, such as pick-up location and contact details, may be processed on a contractual basis, whereas continuous tracking outside active trips, the recording of consumer habits, or unrelated financial profiling requires a separate lawful basis. Where such processing is made a condition of access through bundled consent, its voluntariness is doubtful, and data protection law and contract law must prevent consensualism from legitimising processing that the weaker party cannot meaningfully refuse (Karjalainen, 2022).

Not every transfer of personal data is consideration. Data strictly necessary for performance must be distinguished from additional collection, behavioural profiling, monetisation, and excessive or secondary processing. Access to data must, in turn, be distinguished from consent and from a transfer

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

of rights. Providing data does not transfer the data subject's rights under Articles 5 to 13 of the Personal Data Protection Law, so personal data cannot be sold like property. Directive (EU) 2019/770 nonetheless covers contracts in which consumers provide personal data for digital services, except where the data are processed only to supply the service or meet legal requirements, an exception mirroring the necessity distinction proposed here (Bachelet, 2024).

On this basis, personal data may acquire the character of an additional economic consideration where their processing extends beyond what the transport service strictly requires and generates independent commercial value for the platform, for instance through marketing, personalised promotions, cross-service profiling, or sharing with affiliates, a threshold that must be assessed case by case. Commutative justice demands a balance between the performance rendered and the consideration received (Aristotle, 2009); where the threshold is met, consumers pay through both the fare and their data, while the terms may allocate the risks attached to those data to them (W. Zhang & Zhong, 2022).

The right to privacy has long been recognised as a fundamental human right in international human rights law (Hariz et al., 2026). Application designs that grant driver-partners access to personal phone numbers, home addresses, and daily routines create a foreseeable risk of misuse after the trip, although its frequency is an empirical question beyond this normative study. Legally, Article 35 of the Personal Data Protection Law requires technical and operational measures proportionate to the risks of processing, and encryption, number masking, and time-limited access are recognised means of implementing privacy by design, as reflected in Article 25 of the General Data Protection Regulation.

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

When a loss occurs, the legal consequences of an exoneration clause must be stated precisely. First, a standard clause that transfers the business actor's liability, or that is difficult to read or understand, is void by operation of law (*nietig*) under Article 18 paragraphs (1) to (3) of the Consumer Protection Law (Hosnah et al., 2025). Second, a clause that is not void under Article 18 may still be unenforceable insofar as it purports to exclude mandatory controller obligations, and an ambiguous clause must be interpreted against its drafter under Article 1349 of the Civil Code. Third, nullity is partial: Article 18 paragraph (4), which requires business actors to adjust their standard clauses, presupposes that the contract survives. Fourth, the contract as a whole fails only if an essential requirement under Article 1320 of the Civil Code is affected, which is not ordinarily the case. Clauses that allocate risk legitimately, such as excluding liability for losses caused solely by a user's own disclosure of account credentials, may remain valid.

Driver-partners occupy a distinct position within this ecosystem. The debate on whether their relationship with providers constitutes employment or partnership, including the role of algorithmic management (Cameron, 2024), is significant but lies beyond the scope of this study (Satria, 2025). For data protection purposes, they act as data subjects, contracting parties, and operational users. As data subjects, they provide identity documents, licensing documents, vehicle registration, banking data, and periodic facial biometric verification. Biometric and personal financial data are specific personal data under Article 4 paragraph (2) of the Personal Data Protection Law and therefore warrant heightened protection, which must be translated into concrete safeguards governing how such data are collected, transferred, and relied upon rather than remaining a matter of formal classification (Abdillah et al., 2026). The automated allocation of orders or imposition of suspensions also engages

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

the right to object to decisions based solely on automated processing under Article 10 of the Personal Data Protection Law, an area in which legal oversight of digital platforms remains notably weak (Kadolkar et al., 2025; Muthoifin et al., 2026).

As contracting parties, driver-partners face non-negotiable terms that raise the same concerns of commutative justice as those affecting consumers; as operational users, they access passenger data within an environment designed by the provider and are themselves exposed to fraud such as fake orders. Distributive justice asks whether these risks are borne by the party best placed to control them, while procedural justice requires transparent explanations of automated decisions, accessible complaint channels, and impartial dispute resolution (Stewart & Williams, 2023).

Exoneration clauses also have systemic effects: where standard contracts shift breach-related losses to users, providers' incentives to invest in an Information Security Management System against data manipulation, phishing, and application exploits are reduced (Teichmann & Wittmann, 2023).

The General Data Protection Regulation likewise keeps controllers responsible for demonstrating compliance under Articles 5(2) and 24 (Karjalainen, 2022) and, through Article 7(4), scrutinises consent bundled with contract performance. Article 20 of the Personal Data Protection Law already has a comparable structure; what remains is sectoral harmonisation through revision of Minister of Transportation Regulation Number 118 of 2018.

Enforcement requires identifying the appropriate institutions. Judicial review before the Supreme Court concerns the validity of regulations below statute, such as Minister of Transportation Regulation Number 118 of 2018 (Arifin, 2021), and does not directly invalidate private contract clauses. Such clauses are instead assessed through three channels. The first is civil litigation,

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

which can increasingly be conducted through electronic court services and in which a court may declare a clause void under Article 18 paragraph (3) of the Consumer Protection Law, including through a class action under Article 46. The second is the Consumer Dispute Settlement Body, which also supervises standard clauses under Article 52. The third is administrative supervision under Article 30 of the Consumer Protection Law and Article 57 of the Personal Data Protection Law. Violations of Article 18 also attract criminal sanctions under Article 62 of the Consumer Protection Law.

C. An Integrated Digital Transportation Data Governance Framework: Cybersecurity as a New Regulatory Architecture

Cyberattacks on digital transportation now extend beyond static data to navigation systems, pick-up points, and fare algorithms. Mobility-as-a-service ecosystems are vulnerable at the network, platform, and data management levels. Weak points include interception between driver applications and servers, gaps in the Application Programming Interfaces linking payment, identity verification, and tracking, and storage across third-party servers without uniform encryption; as a result, a single supply-chain failure can escalate into a large-scale breach (Alderete Peralta et al., 2024).

Minister of Transportation Regulation Number 118 of 2018 has not kept pace with these threats. It prioritises fleet roadworthiness, operational zones, and licensing and addresses system security only in general terms, leaving investment in cyber defence to each provider's discretion. Breach notification already exists under Article 46 of the Personal Data Protection Law, but it is not integrated into sectoral supervision, so the transportation regulator does not systematically receive information on incidents. Table 3 maps this gap.

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Table 3. Comparison between the Current Regulatory Paradigm and the Proposed Policy Framework for Digital Transportation Regulation

Aspect	PM 118/2018 (Currently in Force)	Proposed Policy Framework
Primary regulatory focus	Fleet physical roadworthiness, operational zones, administrative licensing	Integrated information risk management alongside transport safety
Cybersecurity obligation	Declaratory in nature (Article 31), without technical parameters	Risk-based ISMS requirements; ISO/IEC 27001 certification for high-risk providers
Liability of application providers	Not addressed	Enhanced accountability under existing law; strict liability for defined high-risk processing (*de lege ferenda*)
Contract terms	Not addressed	Review of data-related exoneration clauses as part of licence supervision
Incident-reporting obligation	Not integrated into the sectoral regime (notification exists under Article 46 of the PDP Law)	Article 46 notifications transmitted to the Ministry of Transportation and considered in licence evaluation
Risk assessment for new features	No sectoral mechanism	Data protection impact assessment (DPIA) under Article 34 of the PDP Law submitted before launching high-risk features
Supervisory institution	A single regulator, the Ministry of Transportation	Coordinated supervision with an explicit allocation of authority

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Aspect	PM 118/2018 (Currently in Force)	Proposed Policy Framework
Sanctions	Tiered administrative sanctions without a financial basis	Sectoral licence consequences coordinated with PDP Law administrative fines (up to 2% of annual revenue)

Source: Compiled by the authors, 2026, based on Minister of Transportation Regulation Number 118 of 2018 and Law Number 27 of 2022

Several of these elements, such as breach notification, impact assessments, and revenue-based fines, already exist in the Personal Data Protection Law; the framework's contribution lies in integrating them into transportation licensing, calibrating them to risk, and clarifying the liability consequences of non-compliance.

The future regulatory framework (*ius constituendum*) should be grounded in information risk management. An Information Security Management System secures information assets through risk management processes, and ISO/IEC 27001 structures it around the confidentiality, integrity, and availability of information (Kitsios et al., 2023). Such a system requires organisational policy, technical procedures, and human resource capability, including asset mapping, risk evaluation, incident and continuity management, and access controls that restrict drivers to the information essential for completing the trip (Chavez et al., 2024).

Mandatory certification must, however, be justified through proportionality and risk-based regulation, which can reconcile legal certainty with fairness only where risk tiers and the division of authority are clearly defined (Suhartana et al., 2025). Indonesia's experience with risk-based business licensing under the Job Creation Law shows that unclear risk criteria and the danger of regulatory capture must be addressed at the design stage (Hariyanto,

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

2022). Digital governance tools should be designed so that the necessity and proportionality of each obligation can be verified, an approach described in other Indonesian regulatory fields as proportionality by design. A uniform obligation would impose substantial costs on smaller providers whose processing presents limited risk and could become a barrier to market entry. Obligations should therefore be calibrated primarily to processing risk, measured by the number of data subjects, the categories of data processed (particularly biometric and financial data), and the intensity of processing. The proposed tiered scheme is set out in Table 4.

Table 4. Tiered, Risk-Based Information Security Management System Certification Scheme

Risk tier	Indicative criteria	Compliance obligation
Tier 1: High risk	Large-scale processing (e.g., millions of active users), specific personal data such as biometric or financial data, continuous geolocation tracking or profiling	ISO/IEC 27001 certification by an accredited body, periodic surveillance audits, and a DPIA before launching high-risk features
Tier 2: Medium risk	Regional operations, moderate user base, no specific personal data beyond what is necessary for the service	Baseline security controls aligned with ISO/IEC 27001, self-assessment verified by periodic audit, and a DPIA where Article 34 of the PDP Law applies
Tier 3: Low risk / start-up	Limited user base and limited data categories	Transition period, baseline security controls, and technical mentoring

Source: Compiled by the authors, 2026

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Precise tier thresholds should be set by implementing regulation, and certification bodies should be accredited by the National Accreditation Committee to prevent conflicts of interest.

A revision of Minister of Transportation Regulation Number 118 of 2018 should incorporate the data protection principles of Law Number 27 of 2022 and add tier-appropriate cybersecurity requirements to licensing. Article 34 of the Personal Data Protection Law already requires a data protection impact assessment where processing presents a high potential risk to data subjects (Metin et al., 2026), and Indonesian scholarship has recommended making such assessments a statutory precondition for large-scale processing, including that of vulnerable data subjects. Sectoral regulation should require providers to submit the assessment to the regulator before launching features involving continuous location processing, behavioural profiling, or drivers' biometric data, making risk assessment a prior rather than reactive stage. Both instruments should also use consistent definitions of data subject, personal data, and data processing, since overlapping statutes that blur the allocation of responsibility tend to produce fragmented protection (Hamzah et al., 2026).

Privacy by design and by default should become legal norms in ministerial regulation, consistent with Article 25 of the General Data Protection Regulation, so that protection is built into application architecture from the design stage (Metin et al., 2026). Encryption and phone number masking should be baseline requirements of operational fitness. Failure to implement a legally required measure would breach a statutory obligation; such a breach would serve as evidence of fault under Article 1365 of the Civil Code and support the presumption proposed in Section III.A. Periodic independent audits should test whether default settings genuinely minimise collection, with a reasonable transition period, such as 18 months, for existing software.

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Digital transportation governance also suffers from institutional fragmentation. The Ministry of Transportation lacks the capacity and jurisdiction to audit providers' computing infrastructure, and uncoordinated authorities tend to produce overlapping or contradictory rules (Anggono et al., 2025; OECD, 2026). Oversight becomes effective when the overseeing body has structured access to the data of the supervised entity and the body's findings trigger a mandatory, time-bound duty to respond. A clear allocation of authority among organs of government is a recurring precondition for effective administration in Indonesia, and weak inter-agency cooperation has repeatedly hampered the implementation of otherwise adequate rights-protective regulation (Hariyanto, Meidina, et al., 2024). The framework therefore calls for coordinated supervision by the Ministry of Transportation, the Ministry of Communication and Digital Affairs, and the personal data protection institution established under Articles 58 to 61 of the Personal Data Protection Law, with an explicit allocation of authority. The institution enforces controller obligations and imposes administrative sanctions, while the Ministry of Transportation links compliance to the grant, renewal, suspension, and revocation of licences, supported by a joint incident information-sharing protocol and auditors competent in law and cybersecurity engineering.

Enforcement instruments must also deter, since the effectiveness of data protection regimes depends more on institutional capacity and enforcement than on the strictness of the law (Palupy et al., 2026). The written warnings, licence suspension, and revocation under Minister of Transportation Regulation Number 118 of 2018 should be applied consistently to providers that fail to secure user data. Article 57 of the Personal Data Protection Law already provides for administrative fines of up to 2% of annual revenue, comparable to Article 83 of the General Data Protection Regulation (Lintvedt, 2022). The

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

proposal is therefore to coordinate the two regimes so that a violation established by the data protection institution has consequences for the operating licence, bearing in mind that fines below the gain from non-compliance become a foreseeable operational cost. Formal rules, moreover, deliver protection only where institutional capacity, transparency, and accountability mechanisms are built alongside them (Hariyanto et al., 2025).

Sanctions should be proportionate to the severity of the violation, the number of affected data subjects, compliance history, and good faith, with permanent revocation as the *ultimum remedium*. Article 46 notifications should be transmitted simultaneously to the Ministry of Transportation and considered in licence evaluation. An independent complaint channel for consumers and driver-partners should complement these measures, protected by a firewall ensuring that complaint data are not used against the complainant, since fear of such repurposing deters vulnerable users from digital mechanisms formally available to them (Zakiyah et al., 2026).

IV. CONCLUSIONS

Synchronising Minister of Transportation Regulation Number 118 of 2018 with Law Number 27 of 2022 places data protection obligations on application providers both as Application Companies and as personal data controllers, regardless of their characterisation as transport operators. This does not establish strict liability under existing law, but it strengthens platform accountability through the reversed burden of proof for consumer claims under Articles 19 and 28 of the Consumer Protection Law and the controller obligations of the Personal Data Protection Law, while strict liability remains a *de lege ferenda* option for high-risk processing. Exoneration clauses that transfer the provider's liability are void by operation of law without invalidating the

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

whole contract. Personal data become an additional economic consideration where their processing exceeds what the transport service requires, so shifting their risks to consumers and driver-partners is incompatible with commutative justice.

The study therefore proposes an Integrated Digital Transportation Data Governance Framework built on regulatory integration, platform accountability, contractual justice, and cybersecurity governance, which incorporates existing Personal Data Protection Law instruments into transportation licensing through risk-based security certification, prior impact assessments, privacy by design, and coordinated supervision. As a normative study, it does not empirically assess the framework's effectiveness or platforms' actual security practices, which further research through technical audits, case analysis, and user studies should address.

BIBLIOGRAPHY

Abdillah, K., Maylissabet, M., & Burhani, N. (2026). Direct-to-Consumer DNA Testing and Nasab in Indonesia: Genetic Privacy and Evidence in Comparative Perspective. *Journal of Law and Digital Civilization*, *1*(2), 97–114. https://doi.org/10.66277/jldc.v1i2.161

Agung, S. F. A. T., & Nasution, M. I. P. (2023). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Di E-Commerce. *Jurnal Ekonomi Manajemen Dan Bisnis (JEMB)*, *2*(1), 5–7. https://doi.org/10.47233/JEMB.V2I1.915

Alderete Peralta, A., Balta-Ozkan, N., & Li, S. (2024). The road not taken yet: A review of cyber security risks in mobility-as-a-service (MaaS) ecosystems and a research agenda. *Research in Transportation Business & Management*, *56*, 101162. https://doi.org/10.1016/J.RTBM.2024.101162

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

American Law Institute. (1977). *Restatement (Second) of Torts*. American Law Institute Publishers.

Anggono, B. D., Wahanisa, R., Sari A.P, A. O. V. P., & Adiyatma, S. E. (2025). Interrogating the Legal Foundations of Digital Transformation: Balancing Economic Growth and Social Welfare in the Era of Disruption. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, *8*(1), 191–211. https://doi.org/10.24090/volksgeist.v8i1.12211

Anwar, A. N., Ridwan, U., Qudsiyah, L., Yanti, I., & Sibawaih, I. (2026). Generative Artificial Intelligence and Copyright Law: Rethinking Intellectual Property Protection in the Digital Era. *Subsidiarity: Journal of Law and Technology Policy*, *1*(1). https://e-journal.anharhariz.org/index.php/subsidiarity/article/view/184

Arifin, F. (2021). Pengujian Peraturan Kebijakan dalam Sistem Peradilan di Indonesia. Litigasi, 22(1), 133–156. https://doi.org/10.23969/litigasi.v22i1.3751

Aristotle. (2009). *The Nicomachean Ethics (W. D. Ross, Trans.)*. Oxford University Press.

Audina Sukmawan, Y., Damayanti, D., HBasri, J., & Selatan, K. (2025). Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum. *Notary Law Journal*, *4*(3), 114–128. https://doi.org/10.32801/NOLAJ.V4I3.116

Bachelet, V. (2024). 'Pay-or-Consent' and Emerging Trends in Digital Contract Law. *European Review of Private Law*, *32*(5), 773–802. https://doi.org/10.54648/ERPL2024047

Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Gema Keadilan*, *7*(1), 20–33. https://doi.org/10.14710/GK.2020.7504

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Cameron, L. D. (2024). The Making of the "Good Bad" Job: How Algorithmic Management Manufactures Consent Through Constant and Confined Choices. *Administrative Science Quarterly*, *69*(2), 458–514. https://doi.org/10.1177/00018392241236163

Chavez, S., Anahue, J., & Ticona, W. (2024). Implementation of an ISMS Based on ISO/IEC 27001:2022 to Improve Information Security in the Internet Services Sector. *Proceedings of the 14th International Conference on Cloud Computing, Data Science and Engineering, Confluence 2024*, 184–189. https://doi.org/10.1109/CONFLUENCE60223.2024.10463392

Desril, R., & Santoso, M. A. (2026). Legal Protection in App-Based Transportation Partnerships and Consumers in Indonesia. *Kosmik Hukum*, *26*(1), 202–216. https://doi.org/10.30595/KOSMIKHUKUM.V26I1.28769

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39–57. https://doi.org/10.23887/GLR.V5I1.2237

Findrikova, D., & Kubina, M. (2026). Implementation of Information Security Management System in Transport Company. *Transportation Research Procedia*, *93*, 916–922. https://doi.org/10.1016/J.TRPRO.2025.12.023

Firdaus, M. (2025). Dialektika Keadilan, Kepastian, Kemanfaatan Hukum dalam Perspektif Gustav Radbruch pada Hukum Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik*, *3*(1), 357–367. https://doi.org/10.62379/QY4B6Z80

Guggenberger, N. (2025). Consent as Friction. *Boston College Law Review*, *66*(2), 353–421. https://doi.org/10.70167/CHOQ9209

Hamzah, A. S., Husni, L., & Arba, A. (2026). Harmonizing Labor and Anti-Trafficking Laws for the Protection of Indonesian Migrant Workers: Toward Legal Certainty and Substantive Justice. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, *9*(2), 397–422. https://doi.org/10.24090/volksgeist.v9i2.15939

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Hariyanto, H. (2022). Risk-Based Business License and Problems Arising After the Job Creation Act. *Jurnal IUS Kajian Hukum dan Keadilan*, *10*(2), 354–366. https://doi.org/10.29303/ius.v10i2.1082

Hariyanto, H., Meidina, A. R., & Azizah, M. (2024). Decentralization and the Fulfilments of Children's Rights: Challenges and Opportunities for Local Government in Indonesia. *Lex Scientia Law Review*, *8*(2), 677–706. https://doi.org/10.15294/lslr.v8i2.14373

Hariyanto, H., Yeyeng, A. T., Kapugu, B. A., Arowosaiye, Y. I., & Tajuddin, M. S. (2025). Democratization of Village Autonomy in the Construction of Indonesian Administrative Law: Is It Possible? *Jurnal Media Hukum*, *32*(2), 190–209. https://doi.org/10.18196/jmh.v32i2.25216

Hariz, H. S. S., Kunarti, S., & Zaman, A. R. B. (2026). Digital Surveillance and the Right to Privacy: A Comparative Study between Indonesia and the European Union. *Subsidiarity: Journal of Law and Technology Policy*, *1*(1). https://e-journal.anharhariz.org/index.php/subsidiarity/article/view/181

Hosnah, A. U., Latif, N., Juliandi, A., Desiana, A. R., & Ma'aruf, R. M. I. (2025). Analisis Perlindungan Data Pribadi dalam Implementasi Undang-Undang Nomor 27 Tahun 2022 di Era Artificial Intelligence. *QAWIUN: Jurnal Penelitian Dan Pengabdian Masyarakat*, *1*(2).

Kadolkar, I., Kepes, S., & Subramony, M. (2025). Algorithmic management in the gig economy: A systematic review and research integration. *Journal of Organizational Behavior*, *46*(7), 1057–1080. https://doi.org/10.1002/JOB.2831

Karjalainen, T. (2022). All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm. *European Data Protection Law Review*, *8*(1), 19–30. https://doi.org/10.21552/EDPL/2022/1/6

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Data in the IT Sector. *Sustainability*, *15*(7), 5828. https://doi.org/10.3390/SU15075828

Lintvedt, M. N. (2022). Putting a price on data protection infringement. *International Data Privacy Law*, *12*(1), 1–15. https://doi.org/10.1093/IDPL/IPAB024

Made, I., Praditya, D. A., Gede, B., Rama, A., Agung, A., Ngurah, A., Gorda, S. R., Gede, I., & Kurniawan, A. (2025). Perlindungan Hukum Data Pribadi Pengguna Layanan Transportasi Digital Dalam Perspektif Perbandingan Hukum. *Jurnal Yustitia*, *19*(2), 13–30. https://doi.org/10.62279/YUSTITIA.V21I2.1623

Made, N., Putri, D. G., Luh, N., Mahendrawati, M., & Ujianti, P. (2024). Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Preferensi Hukum*, *5*(2), 240–245. https://doi.org/10.22225/jph.5.2.2024.240-245

Mariyam, S. (2019a). Bentuk Perusahaan Jasa Angkutan Sewa Khusus menurut Peraturan Menteri Perhubungan Nomor 118 Tahun 2018. *Jurnal Ilmiah Hukum dan Dinamika Masyarakat*, *17*(1). https://doi.org/10.56444/HDM.V17I1.1282

Mariyam, S. (2019b). Tinjauan Yuridis Jasa Angkutan Umum dengan Aplikasi Berbasis Teknologi Informasi (Perspektif Hukum Bisnis). *Jurnal Ilmiah Hukum dan Dinamika Masyarakat*, *16*(2). https://doi.org/10.56444/HDM.V16I2.1009

Mariyam, S., Febriharini, M. P., Krismiyarsi, & Karyono, H. (2026). Between Efficiency and Risk: Data Security in Digital Transportation and the Legal Liability of Platform Providers. *Jurnal Ilmu Hukum Tambun Bungai*, *11*(1), 737–749. https://doi.org/10.61394/JIHTB.V11I1.634

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Mashchenko, O., & Radiev, D. (2023). Institutional Environment of the Digital Economy Sector. *Baltic Journal of Economic Studies*, *9*(5), 169–175. https://doi.org/10.30525/2256-0742/2023-9-5-169-175

Metin, B., Yey, N. E., & Wynn, M. (2026). Addressing Data Protection Impact Assessment (DPIA) Implementation Challenges in AI-Driven Digitalisation: A Systematic Review and PDCA-Based Governance Framework. *Information*, *17*(7), 679. https://doi.org/10.3390/INFO17070679

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. Microsoft Corporation.

Muthoifin, M., Elbanna, M., & Afiyah, I. (2026). Legal Oversight in Digital Marketplaces: A Bibliometric Analysis and Systematic Literature Review of Research Trends and Gaps. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, *9*(1), 145–174. https://doi.org/10.24090/volksgeist.v9i1.15587

Novalius, F. (2017, May 12). *Survei YLKI, 84,1% Masyarakat Pilih Transportasi Online.* Okezone Economy. https://economy.okezone.com/read/2017/05/12/320/1689169/survei-ylki-84-1-masyarakat-pilih-transportasi-online

OECD. (2026). Towards international coherence of cybersecurity regulations. *OECD Digital Economy Papers*. https://doi.org/10.1787/BD1F199A-EN

Olasehinde, D. O., Bamisile, O., Ejiyi, C. J., Zhang, G., Cai, D., Li, J., Wei, L., & Huang, Q. (2026). Cybersecurity in cyber-physical power systems: analyzing vulnerabilities, threats, and control structures. *Cluster Computing*, *29*(3), 133. https://doi.org/10.1007/S10586-025-05894-W

Palupy, H. E., Nawing, R., & Susantijo, S. (2026). Personal Data Protection Governance in the Asia Pacific Region: A Review of the Scope, Effectiveness, and Legal Challenges. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, *9*(1), 197–225. https://doi.org/10.24090/volksgeist.v9i1.15362

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Rejeki, S. K. (2026). Analisis Yuridis terhadap Perlindungan Hak Privasi dalam Komunikasi Digital Berdasarkan Undang-Undang Pelindungan Data Pribadi di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 7607–7621. https://doi.org/10.61104/ALZ.V4I2.5682

Sanjaya, S., Alfani, I. P., & Sinaga, S. (2026). Keabsahan Kontrak Elektronik dalam Hukum Perdata Indonesia: Tantangan dan Perlindungan Hukum. *Jurnal Hukum Mimbar Justitia*, *12*(1), 232–250. https://doi.org/10.35194/JHMJ.V12I1.6135

Sari, D. P., Safa, M. S., & Fahlevi, A. R. (2026). Perlindungan Hukum Konsumen dalam Transaksi E-Commerce di Indonesia: Perspektif Hukum Perdata dan Undang-Undang Perlindungan Konsumen. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *5*(1), 6311–6318. https://doi.org/10.31004/riggs.v5i1.6942

Satria, I. G. S. (2025). Perlindungan Hak Pekerja Gig Economy melalui Perspektif Hukum Ketenagakerjaan. *Nomos: Jurnal Penelitian Ilmu Hukum*, *5*(1), 127–134. https://doi.org/10.56393/NOMOS.V5I1.2723

Sepriadi, O., Zulfikar, P., Ghifari, S. Al, Budi, U., & Ridwan. (2026). Hubungan Hukum Kontrak Elektronik dengan Keamanan Transaksi Digital. *Berajah Journal*, *6*(3), 867–873. https://doi.org/10.47353/BJ.V6I3.534

Stewart, A., & Williams, P. (2023). Regulating the Fairness of Work Contracts in the Gig Economy. *Federal Law Review*, *51*(4), 466–486. https://doi.org/10.1177/0067205X231205049

Suhartana, L. W. P., Asikin, Z., Haq, L. M. H., & Azizah, M. (2025). Risk-Based Mining Investment in the Framework of Fair Legal Certainty. *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi*, *8*(1), 63–85. https://doi.org/10.24090/volksgeist.v8i1.12894

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274

Teichmann, F. M. J., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime*, *30*(6), 1491–1498. https://doi.org/10.1108/JFC-04-2022-0093

Wijaya, E., Rahardiansyah, T., & Notoprayitno, M. I. (2025). Dimensi Sosio-Legal dalam Pengaturan Transportasi Publik Berbasis Aplikasi. *MIMBAR KEADILAN: Jurnal Ilmu Hukum*, 209–216. https://doi.org/10.5139.vol1iss6pp209

Yuspin, W., Rajput, T., Bal, A. B., Wardiono, K., & Absori. (2024). The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle. *BESTUUR*, *12*(1), 49–68. https://doi.org/10.20961/BESTUUR.V12I1.89742

Zakiyah, N., Ulum, B., Rahmat, H., & Ahmad, A. R. bin. (2026). Digital Registration and the Invisible Child: Protecting Children of Unregistered Migrant Marriages in Malaysia. *Journal of Law and Digital Civilization*, *1*(2), 115–134. https://doi.org/10.66277/jldc.v1i2.31

Zhang, J. (2024). Analysis and Solution of the Governance Dilemma of Infringement of Car-Hailing Platforms under Sharing Economy. *Frontiers in Business, Economics and Management*, *15*(2), 107–110. https://doi.org/10.54097/9G1AM937

Zhang, W., & Zhong, S. (2022). Data Legal Supervision of Online Car-Hailing Platform Based on Big Data Technology and Edge Computing. *Wireless Communications and Mobile Computing*, *2022*(1), 5298152. https://doi.org/10.1155/2022/5298152

Zhou, Z. (2022). Research on Legal Issues in Safety Incidents of Ride-hailing and Their Coping Mechanisms. *Academic Journal of Humanities & Social Sciences*, *5*(4), 95–105. https://doi.org/10.25236/AJHSS.2022.050416

Copyright © 2026, **Jurnal LITIGASI**, e-ISSN: 2442-2274