

REVISTA DE DIREITO INTERNACIONAL
BRAZILIAN JOURNAL OF INTERNATIONAL LAW

Corporate accountability for labour data protection in EU-ASIA FTAs: A comparative analysis of TSD chapters and national compliance in ASEAN

Responsabilização empresarial pela proteção de dados dos trabalhadores nos acordos de livre comércio UE-Ásia: Uma análise comparada dos capítulos sobre comércio e desenvolvimento sustentável e do cumprimento das normas nacionais na ASEAN

Hoang Trung Hieu

Nguyen Thi Minh Phuong

VOLUME 23 • N. 2 • 2026

Corporate accountability for labour data protection in EU-ASIA FTAs: A comparative analysis of TSD chapters and national compliance in ASEAN*

Responsabilização empresarial pela proteção de dados dos trabalhadores nos acordos de livre comércio UE-Ásia: Uma análise comparada dos capítulos sobre comércio e desenvolvimento sustentável e do cumprimento das normas nacionais na ASEAN

Hoang Trung Hieu**

Nguyen Thi Minh Phuong***

Abstract

As the European Union continues to ‘export’ its high social and environmental standards through the Trade and Sustainable Development (TSD) chapters in new-generation FTAs like the EVFTA, EUSFTA, and the proposed EU-Thailand FTA, a new regulatory frontier has emerged in Asia: corporate accountability for employee data. While traditional labour disputes focused on wages and working hours, the rapid ‘platformisation’ and ‘digitalisation’ of labour markets have shifted regulatory attention toward algorithmic management, workplace surveillance, and employee data protection.

This research examines corporate accountability for labour-data protection as an emerging issue of sustainable trade governance in EU-Asia economic relations. It argues that, although Trade and Sustainable Development (TSD) chapters in the European Union’s new-generation free trade agreements do not expressly regulate labour data, they nonetheless reshape the normative structure of trade by embedding labour protection, non-regression, monitoring, and participatory implementation mechanisms within market integration. Drawing on the Brussels Effect, the article investigates how these trade-linked normative pressures interact with domestic legal frameworks governing employee data.

Using a functional comparative approach, the article analyses Singapore, Thailand, Malaysia, and Vietnam against two criteria: the enforcement and accountability mechanisms and the influence of international trade and market pressures on regulatory development, in domestic personal data protection regimes. The comparative analysis finds significant variation in the degree of protection and enforcement across the four jurisdictions, and the demonstration that, although EU trade agreements do not directly regulate labour data, they contribute to a broader process of legal adaptation by reinforcing expectations of responsible corporate data governance. The arti-

* Received on: 15/05/2026
Approved on: 13/10/2026

** Hoang Trung Hieu, Ph.D., is a Lecturer at the Faculty of Civil Law, Ho Chi Minh City University of Law, Vietnam. His teaching and research interests include labour law, contract law, personal data protection, legal education, and legal issues arising from digital transformation and emerging technologies.
E-mail: hthieu@hcmulaw.edu.vn

*** Nguyen Thi Minh Phuong, LL.M., is a doctoral candidate at the University of Waikato, New Zealand, and a Lecturer at the Faculty of International Law, Ho Chi Minh City University of Law, Vietnam. She holds a Master’s degree in International Business Law from Université Paris-Panthéon-Assas (Paris II), France. Her teaching and research interests include public international law, international environmental law, and the law of the sea. She is also a member of the Henri Capitant Association of Friends of French Legal Culture.
E-mail: ntmphuong_qte@hcmulaw.edu.vn

cle concludes by proposing that labour-data protection should be more explicitly integrated into the evolving framework of sustainable trade governance and future EU-ASEAN economic relations to balancing economic growth with the protection of fundamental digital rights in labour relations.

Keywords: *corporate accountability, labour data, FTA, TSD chapter, ASEAN*

Resumo

À medida que a União Europeia continua a “exportar” seus elevados padrões sociais e ambientais por meio dos capítulos sobre Comércio e Desenvolvimento Sustentável (CDS) dos acordos de livre comércio de nova geração, como os celebrados com o Vietnã e Singapura e o proposto acordo com a Tailândia, uma nova fronteira regulatória emerge na Ásia: a responsabilização empresarial pelo tratamento dos dados dos trabalhadores. Enquanto os conflitos trabalhistas tradicionais se concentravam nos salários e na jornada de trabalho, a rápida plataformização e digitalização dos mercados de trabalho deslocou a atenção regulatória para a gestão algorítmica, a vigilância no ambiente de trabalho e a proteção de dados dos trabalhadores. Esta pesquisa examina a responsabilização empresarial pela proteção de dados dos trabalhadores como uma questão emergente da governança do comércio sustentável nas relações econômicas entre a União Europeia e a Ásia. Sustenta que, embora os capítulos sobre CDS dos acordos de livre comércio de nova geração da União Europeia não regulem expressamente esses dados, eles reconfiguram a estrutura normativa do comércio ao incorporar a proteção trabalhista, a não regressão, o monitoramento e os mecanismos participativos de implementação à integração dos mercados. Com base no Efeito Bruxelas, o artigo investiga como essas pressões normativas vinculadas ao comércio interagem com os regimes jurídicos nacionais aplicáveis aos dados dos trabalhadores. Mediante uma abordagem comparativa funcional, o artigo analisa os regimes nacionais de proteção de dados pessoais de Singapura, Tailândia, Malásia e Vietnã segundo dois critérios: os mecanismos de aplicação das normas e de responsabilização; e a influência do comércio internacional e das pressões de mercado sobre o desenvolvimento regulatório. A análise comparada identifica variações significativas no grau de proteção e na apli-

cação das normas nas quatro jurisdições e demonstra que, embora os acordos comerciais da União Europeia não regulem diretamente os dados dos trabalhadores, contribuem para um processo mais amplo de adaptação jurídica ao reforçar as expectativas de uma governança empresarial responsável dos dados. O artigo conclui propondo a integração mais explícita da proteção de dados dos trabalhadores ao quadro em evolução da governança do comércio sustentável e às futuras relações econômicas entre a União Europeia e a ASEAN, de modo a conciliar o crescimento econômico com a proteção dos direitos digitais fundamentais nas relações de trabalho.

Palavras-chave: responsabilização empresarial; dados dos trabalhadores; acordos de livre comércio; capítulos sobre comércio e desenvolvimento sustentável; ASEAN

1 Introduction

International trade law is no longer confined to the reduction of tariffs, the elimination of quotas, or the technical management of market access. In the contemporary global economy, trade agreements increasingly function as governance instruments through which states negotiate the social, environmental and technological conditions under which cross-border commerce takes place.¹ This transformation is closely linked to the rise of the sustainable development agenda and the expansion of the digital economy.

The evolution of the digital world and technological development have added a new stakeholder concern to the corporate social responsibility (CSR) agenda of businesses, privacy and data protection.² While technological adoption is to simplify business processes and increase revenue generation, it also poses far-reaching implications and risks, particularly with data breaches.

¹ James Harrison, ‘Trade Agreements and Sustainability: Exploring the Potential of Global Value Chain (GVC) Obligations’ (2023) 26(2) *Journal of International Economic Law* 199-215; Gregory Messenger, ‘Free Trade Agreements as Sites of Economic Diplomacy: Agreeing Common Standards for Sustainable Development’ (2025) 24(S2) *World Trade Review* 194.

² Joanna van der Merwe and Ziad Al Achkar, ‘Data Responsibility, Corporate Social Responsibility, and Corporate Digital Responsibility’ (2022) 4 *Data & Policy* e12; Vasso Steele, ‘Corporate Social Responsibility, Data Protection and the Right to Privacy’ (2022) 2 *Student Law Journal* 23-43.

As production, services, and labour relations become more data-driven, international trade law is now required to engage with issues that were once treated as peripheral to trade governance, including labour rights, privacy, corporate conduct, and the regulation of digital infrastructures.³ In that sense, the intersection between international trade law, the sustainable development goals (SDGs), and the digital economy reflects a broader normative shift: trade is expected not merely to generate growth, but to do so in a manner consistent with social justice, environmental protection, and technologically responsible governance.

The contemporary evolution of international trade law reflects a structural shift from tariff reduction and market-access liberalization toward the incorporation of increasingly institutionalized obligations relating to sustainable development, labour protection, and responsible business conduct.⁴ Within this normative reorientation, corporate accountability assumes a more central legal function, serving as one of the mechanisms through which trade-linked sustainability commitments are translated into obligations of compliance, due diligence, and demonstrable corporate conduct within domestic and transnational economic governance.⁵

Corporate accountability in Asian jurisdictions has evolved from voluntary philanthropic traditions toward legally recognised obligations embedded in ESG frameworks (Environmental, Social, & Governance) corporate governance codes, and increasingly mandatory disclosure regimes, yet enforcement gaps and institutional capacity deficits persist across the region. International trade law influences the development of corporate accountability through at least three doctrinal pathways: market-access conditionality embedded in trade agreements,⁶ the diffusion of governance models

through international institutional frameworks,⁷ and the growing role of digital trade instruments in shaping domestic regimes of data governance and regulatory autonomy.⁸

This normative reorientation becomes particularly pronounced in the digital economy, where trade governance increasingly intersects with the regulation of data, technological infrastructures, and labour relations. The digital economy has restructured production and labour relations through data-intensive platforms, algorithmic management, and networked infrastructures that render workers' behavioural and performance data a strategic economic asset rather than a merely administrative by-product.⁹ This transformation extends the scope of trade governance beyond market liberalization by creating a stronger need for legal frameworks capable of regulating workplace surveillance, cross-border data flows, and corporate accountability for the protection of labour-data rights.¹⁰

Unlike responsibility and liability, accountability does not have a clear definition in international law. In general, it can be used to describe processes by which corporations can be held to account under international (soft) law.¹¹ Here, in the scope of this article, the term "corporate accountability" denotes enterprises' obligations to organise, explain and demonstrate compliance with applicable data-protection duties and to answer for failures through oversight and remedial mechanisms. Corporate responsibility concerns the substantive duties owed; accountability concerns the procedures through which their fulfilment can be assessed and enforced.

³ Mira Burri and Kholofelo Kugler, 'Regulatory Autonomy in Digital Trade Agreements' (2024) 27(3) *Journal of International Economic Law* 397-423; Mira Burri, 'Digital Trade Law and Human Rights' (2023) 117 *AJIL Unbound* 110-115; Jean-Baptiste Velut, 'Trade Linkages or Disconnects? Labor Rights and Data Privacy in US Digital Trade Policy' (2023) 11(1) *Politics and Governance* 249-260.

⁴ *Id.* 3.

⁵ Lorand Bartels, 'Human Rights and Sustainable Development Obligations in EU Free Trade Agreements' (2013) 40(4) *Legal Issues of Economic Integration*, 297-313.

Cindy Woods, 'Engaging the U.N. Guiding principles on business and human rights: the inter-american commission on human rights & the extractive sector' (2015). *Brazilian Journal of International Law*, 12(2), 570-588. <https://doi.org/10.5102/rdi.v12i2.3572>

⁶ *Id.* 3.

⁷ Fabrizio De Francesco and Edoardo Guaschino, 'Reframing Knowledge: A Comparison of OECD and World Bank Discourse on Public Governance Reform' (2020) 39(1) *Policy and Society* 113-128.

⁸ Neha Mishra and Ana Maria Palacio Valencia, 'Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?' (2023) 31(2) *Asia Pacific Law Review* 489-513; Mira Burri and Kholofelo Kugler, 'Regulatory Autonomy in Digital Trade Agreements' (2024) 27(3) *Journal of International Economic Law* 397-423.

⁹ Valerio De Stefano, 'Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection' (ILO Employment Working Paper No 246, 2018)

¹⁰ International Labour Office, *World Employment and Social Outlook 2021: The Role of Digital Labour Platforms in Transforming the World of Work* (ILO 2021)

¹¹ Bernaz, N. Conceptualizing Corporate Accountability in International Law: Models for a Business and Human Rights Treaty. *Hum Rights Rev* 22, 45-64 (2021). <https://doi.org/10.1007/s12142-020-00606-w>

In this field, corporate accountability protects workers from arbitrary and opaque data practices, compels firms to internalize the risks of digital management,¹² and prevents digital trade gains from being achieved by externalizing social costs onto labour. It also supports trust in cross-border commerce and strengthens the legitimacy of trade governance.¹³

The mandatory requirement for corporate accountability for labour data protection becomes more complex in the context of EU-Asia free trade agreements. Through TSD chapters, labour commitments, and expectations of responsible business conduct, the EU projects sustainability-related norms beyond Europe while formally preserving regulatory autonomy. Even without explicit labour-data provisions, such agreements may still shape domestic reform by strengthening labour institutions, improving enforcement, and linking trade competitiveness to social protection. Therefore, accountability for labour data protection therefore lies at the intersection of trade conditionality, regulatory diffusion, and the Brussels effect, whereby access to the EU market creates incentives for legal convergence.

In practice, the term “labour data” (or “employment data”) does not have the specific definition in the domestic legal framework or in international law as GDPR of the EU. Article 88 of the GDPR governs “employee personal data” and HR data” under its general definition of personal data. For the purposes of this article, from the common regulation in the GDPR or the domestic law on personal data, “labour data” can be defined as personal data relating to an identified or identifiable applicant or worker,¹⁴ processed in connection with recruitment, employment or its termination. It can include personnel records, performance assessments and information generated by workplace monitoring or

algorithmic management.¹⁵ It is a context-specific subset of personal data, which may include sensitive data as classified by the applicable law; performance data constitute only one part of this category.

From the definition of the term “labour-data”, “labour-data protection” refers to the legal safeguards governing this processing and the associated rights and remedies of applicants and workers. Labour data protection should therefore be understood not merely as a privacy issue, but as a trade-and-sustainability issue. Export manufacturing, business-process outsourcing, logistics, and digitally mediated services increasingly rely on intensive processing of worker data. These data shape recruitment, productivity monitoring, welfare administration, workplace access, remote supervision, and compliance auditing across supply chains. Where digital trade rules facilitate data flows without adequate labour and privacy safeguards, competitiveness may come to depend on informational asymmetry and worker vulnerability.

By contrast, requirements concerning purpose limitation, data minimization, security, fairness in automated decision-making, and accessible complaint mechanisms can support more sustainable and rights-compatible forms of economic integration. The governance of labour data is therefore central to the broader question of whether trade law can promote development without undermining human dignity at work.

Against this background, ASEAN offers a productive site for comparative analysis. Its member states combine manufacturing integration, digital transformation, legal pluralism, and active engagement with external trade partners. They face common pressures to modernize labour law, attract investment, facilitate e-commerce,

¹² Antonio Aloisi, ‘Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-discrimination and Collective Rights’ (2024) 40(1) *International Journal of Comparative Labour Law and Industrial Relations* 37-70; Halefom Abraha, ‘Regulating Algorithmic Employment Decisions through Data Protection Law’ (2023) 14(2) *European Labour Law Journal* 172-191.

¹³ James Harrison and others, ‘Labour Standards Provisions in EU Free Trade Agreements: Reflections on the European Commission’s Reform Agenda’ (2019) 18(4) *World Trade Review* 635-657; Marco Bronckers and Giovanni Gruni, ‘Retooling the Sustainability Standards in EU Free Trade Agreements’ (2021) 24(1) *Journal of International Economic Law* 25-51.

¹⁴ ILO Code of Practice on the Protection of Workers’ Personal Data. See more at <https://webapps.ilo.org/static/english/intserv/working-papers/wp062/index.html> (accessed on 10 October 2026)

¹⁵ Article 88 of GDPR specifically isolates data processed “in the employment context” which must cover data for (i) Recruitment and the performance of the contract of employment; (ii) Labour management, planning, and organization of work; (iii) Health and safety at work; (iv) The exercise and enjoyment of rights and benefits related to employment; and (v) The termination of the employment relationship.

The American Data Privacy and Protection Act explicitly creates a definition for “employee data” as a distinct sub-category of covered data, including (i) Information collected by an employer that relates to a job applicant; (ii) Business contact information; (iii) Emergency contact; and (iv) Information necessary to administer benefits.

The International Labour Organisation Code guidelines the list of data that must be regulated as “workers’ personal data” including (i) Medical data and health records; (ii) Biometric data; and (iii) Monitoring data.

and establish credible data-governance frameworks, but they respond through different constitutional structures, regulatory traditions, and institutional capacities. Examining these jurisdictions together helps identify both convergence and divergence in emerging Asian approaches to corporate accountability.¹⁶

The legal problem is how sustainability commitments addressed to states can translate into enforceable corporate duties concerning labour data when TSD chapters do not expressly regulate labour data protection. The problematic here is through which legal and institutional mechanisms, and with what limits, do EU trade commitments and market pressures contribute to corporate accountability for labour-data protection in Singapore, Thailand, Malaysia, and Vietnam? The analysis distinguishes obligations under agreements in force from reform expectations associated with negotiations and from market-driven incentives.

This article argues that the future of sustainable trade in Asia depends not only on inter-state commitments in TSD chapters, but also on their domestic translation into enforceable forms of corporate accountability, particularly where digital technologies restructure labour relations.

This study combines doctrinal legal analysis with functional comparison to examine corporate accountability for labour-data protection in Singapore, Thailand, Malaysia, and Vietnam. These jurisdictions are selected to explore variation in domestic data-protection frameworks and their engagement with EU trade governance, rather than to represent ASEAN. The analysis draws on relevant treaty provisions, national legislation, regulatory guidance, and published enforcement cases, read alongside academic literature. It applies two criteria: the enforcement and accountability mechanisms and the influence of international trade and market pressures on regulatory development, in domestic personal data protection regimes. Under each criterion, the analysis considers the obligations placed on enterprises and their implications for workers' data, including personnel records, workplace monitoring, and algorithmic management. Treaty obligations in force are distinguish-

shed from negotiating objectives and market-driven incentives. The comparison also separates regulatory design from enforcement outcomes.

2 From TSD Chapters to Domestic Reform: EU Influence on Labour-Data Accountability in ASEAN

2.1 Treaty-Based Integration of EU labour data standards

Currently, the international trend is shifting from voluntary commitments (soft law) to mandatory legal obligations (hard law), typically the provisions on Trade and Sustainable Development (TSD) in new-generation free trade agreements such as EVFTA, EUSFTA or EU-Thailand FTA, etc.¹⁷

Among contemporary trade actors, the European Union has been particularly influential in institutionalizing this linkage through the Trade and Sustainable Development (TSD) chapters included in its so-called new-generation free trade agreements. The EU's TSD model embeds commitments relating to labour standards, environmental protection, regulatory non-derogation, and cooperative mechanisms aimed at improving domestic compliance rather than relying solely on traditional retaliatory trade sanctions. The TSD chapter of the EVFTA expressly connects trade relations with the objective of sustainable development and recalls major international instruments such as the ILO Decent Work Agenda and the 2030 Agenda for Sustainable Development, while the EUSFTA similarly includes a dedicated TSD chapter reflecting the EU's view that trade liberalization must be accompanied by sustainability commitments.

More specifically, the EVFTA demonstrates that the legal significance of TSD chapters lies as much in their implementation architecture as in their substantive commitments. Chapter 13 embeds sustainable development within the bilateral trade relationship and supports

¹⁶ Andrew Harding and Mark Sidel (eds), *Central and Southeast Asian Legal Systems* (Cambridge University Press 2021); Asian Development Bank, *Asian Economic Integration Report 2021: Making Digital Platforms Work for Asia and the Pacific* (ADB 2021); Graham Greenleaf, *Asian Data Privacy Laws* (OUP).

¹⁷ Daan van 't Wout, 'The Enforceability of the Trade and Sustainable Development Chapters of the European Union's Free Trade Agreements' (2022) 20 *Asia Europe Journal* 81-98; James Harrison and others, 'Labour Standards Provisions in EU Free Trade Agreements: Reflections on the European Commission's Reform Agenda' (2019) 18(4) *World Trade Review* 635-657.

that objective through a structured institutional design, including a specialised Committee on Trade and Sustainable Development, Domestic Advisory Groups representing independent social and economic stakeholders, a Joint Forum for civil-society dialogue, and a consultation mechanism culminating, where necessary, in a Panel of Experts. Although these procedures do not impose direct sanctions comparable to ordinary trade remedies, they subject labor-related commitments to recurrent scrutiny, reporting, and interpretive development. In that respect, the EVFTA does not expressly regulate labour data, but it nonetheless generates a legal environment in which emerging questions of workplace surveillance, digital compliance, and corporate responsibility may increasingly be framed as matters of sustainable trade governance rather than merely internal managerial discretion.¹⁸

These agreements matter not only because they facilitate market access, but also because they transmit normative expectations regarding labour governance, responsible business conduct, and domestic regulatory autonomy.¹⁹ Data governance accountability refers to the legal and organizational responsibility of entities and decision-makers to ensure that data is managed, protected, and used in compliance with applicable laws and regulatory standards.²⁰ In domestic jurisdictions, data corporate accountability is enforced generally through data protection and consumer protection laws. Accountability can be deemed as the bedrock of digital trust. It ensures that every decision regarding data, from collection to disposal, has a clear owner who is responsible for the legal and ethical outcomes.

The inclusion of TSD chapters in the European Union's new-generation free trade agreements marks a significant development in the legal architecture of trade governance. These chapters do not merely supplement market-access commitments with aspirational references to labour and environmental values. Rather, they institutionalise a distinct normative logic within

trade law, under which liberalisation is increasingly conditioned by continuing commitments to regulatory maintenance, cooperation, monitoring, and review. Although the classical criticism of TSD chapters has been their limited coercive force, their legal significance lies precisely in the fact that they reconstitute the terms on which trade integration is understood to occur: not as a value-neutral process of economic exchange, but as a framework embedded in broader public-regulatory objectives.²¹

From this perspective, the absence of express provisions on labour data should not be taken to imply doctrinal irrelevance. TSD chapters operate not only through direct rule prescription, but also through the diffusion of governance rationalities that reshape the interpretation of domestic regulatory priorities. Once trade agreements require parties to maintain labour protections, refrain from regulatory backsliding, and participate in institutionalised forms of oversight, they generate normative pressure against the treatment of workplace data practices as purely internal matters of managerial discretion. In increasingly digitalised labour markets, the collection, processing, and deployment of worker data are bound up with questions of dignity, autonomy, equality, and risk allocation at work. Those questions sit comfortably within the broader trajectory of sustainable trade governance, even where the relevant treaty text has not yet caught up with the technological specificity of the problem.²²

The analytical significance of this shift is that it moves the discussion beyond the traditional vocabulary of corporate social responsibility. Corporate social responsibility has frequently been articulated in voluntary, ethical, or reputational terms. Corporate accountability, by contrast, denotes a more exacting framework in which enterprises are expected to justify conduct, internalise foreseeable harms, and remain subject to institutional mechanisms capable of evaluating compliance and, where necessary, imposing consequences. In that sense,

¹⁸ Free Trade Agreement between the European Union and the Socialist Republic of Viet Nam, ch 13, arts 13.1-13.2, 13.15-13.17

¹⁹ *Id.* 16.

²⁰ 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 (General Data Protection Regulation) [2016] OJ L119/1, art 5(2); Personal Data Protection Commission Singapore, Guide to Accountability under the Personal Data Protection Act (15 July 2019).

²¹ *Id.* 14.

²² Lorand Bartels, 'Human Rights and Sustainable Development Obligations in EU Free Trade Agreements' (2013) 40(4) *Legal Issues of Economic Integration* 297; Mira Burri and Kholofelo Kugler, 'Regulatory Autonomy in Digital Trade Agreements' (2024) 27(3) *Journal of International Economic Law* 397; Antonio Aloisi, 'Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-discrimination and Collective Rights' (2024) 40(1) *International Journal of Comparative Labour Law and Industrial Relations* 37.

accountability is better suited than CSR to explain how trade-linked sustainability commitments may be translated into domestic obligations governing corporate behaviour, including in relation to the datafication of labour management.²³

This development is particularly important in the ASEAN context, where the European Union's influence often operates less through formal harmonisation than through regulatory diffusion. TSD chapters, together with the wider Brussels Effect, create incentives for states and firms to align domestic governance frameworks with standards that are increasingly treated as conditions of market credibility and legal reliability in transnational commerce. The result is not a simple transplantation of EU law into ASEAN legal systems. Rather, it is a process of selective adaptation, through which labour-data risks are gradually reclassified from private questions of business efficiency into matters of public regulation, sustainable trade legitimacy, and corporate accountability. That reclassification provides the conceptual bridge for understanding why labour-data protection should be analysed not merely as a question of privacy law, but as part of the evolving governance of sustainable trade in Asia.²⁴

Having traced the treaty-based foundations of EU influence, the analysis now shifts to the indirect mechanisms through which that influence is internalized in ASEAN legal orders. This next part examines the Brussels Effect as a key driver of labour-data reform beyond the text of the agreements themselves.

2.2 The Brussels Effect and Labor Data Legal Reform in some ASEAN countries

The Brussels Effect refers to the European Union's ability to shape global regulatory behaviour through the

gravitational force of its internal market. Rather than relying primarily on treaty-based harmonization or classic extraterritorial jurisdiction, the EU often influences foreign firms and legal systems indirectly: market actors that wish to retain access to the European market frequently find it more efficient to adopt EU-compliant standards across their wider operations. As a result, EU regulatory choices may diffuse internationally and become embedded in domestic legal reform abroad. In the context of digital governance, this helps explain why EU rules and regulatory models exert influence in third countries, including ASEAN member states, even where those states have not formally undertaken full legal harmonization with EU law.²⁵

In the Asian context, this dynamic is visible not only in general data protection reform inspired by the GDPR, but also in the broader restructuring of domestic regulatory frameworks around transparency, accountability, risk management, and demonstrable compliance. The result is not simple legal transplantation. Rather, Asian jurisdictions selectively internalize EU-style principles while adapting them to domestic priorities such as developmental governance, digital industrialization, and state-led regulatory oversight.

This regulatory diffusion is reinforced by the TSD chapters in EU free trade agreements with Asian partners. The EVFTA, for example, expressly integrates sustainable development into the bilateral trade relationship, recalls the ILO Decent Work Agenda and the 2030 Agenda, and requires both parties to maintain and continue improving domestic levels of labour and environmental protection.²⁶ Likewise, the EU-Singapore Free Trade Agreement contains a dedicated TSD chapter and reflects the EU's insistence that trade liberalization be accompanied by commitments relating to labour rights, environmental protection, and responsible governance.²⁷ Although these agreements do not impose a single uniform model of data or labour law, they create sustained incentives for legislative and administrative convergence by linking market access, reputational credibility, and participation in global value chains with higher compliance expectations.

²³ Cecilia Navarra, *Corporate Due Diligence and Corporate Accountability* (European Parliamentary Research Service 2020); Archie B Carroll, 'Corporate Social Responsibility: Evolution of a Definitional Construct' (1999) 38(3) *Business and Society* 268; Malika Tamvada, 'Corporate Social Responsibility and Accountability: A New Theoretical Foundation for Regulating CSR' (2020) 5 *International Journal of Corporate Social Responsibility* 1.

²⁴ Bradford, Anu, "The Brussels Effect: How the European Union Rules the World" (2020). Faculty Books. 232. <https://scholarship.law.columbia.edu/books/232> <https://doi.org/10.1093/oso/9780190088583.001.0001>; Free Trade Agreement between the European Union and the Socialist Republic of Viet Nam, ch 13; Free Trade Agreement between the European Union and the Republic of Singapore, ch 12

²⁵ *Id.*, 22.

²⁶ Free Trade Agreement between the European Union and the Socialist Republic of Vietnam, ch 13 'Trade and Sustainable Development', arts 13.1-13.2.

²⁷ Free Trade Agreement between the European Union and the Republic of Singapore, ch 12 'Trade and Sustainable Development'.

For labour-data governance in particular, the importance of the Brussels Effect lies in its indirect but powerful capacity to reframe what counts as acceptable corporate conduct. Once access to EU markets, investment relationships, or contractual integration with European firms depends upon credible safeguards for privacy, workplace monitoring, data security, and due diligence, Asian lawmakers and regulators face pressure to modernize domestic legal regimes. This helps explain why reforms in countries such as Singapore, Thailand, and Vietnam increasingly emphasize accountability-based governance, cross-border transfer controls, internal compliance systems, and risk-based supervision. In this sense, EU influence operates through both *de facto* market mechanisms and *de jure* treaty commitments: the former pushes firms to globalize EU standards operationally, while the latter encourages states to revise national laws in ways that make those standards institutionally sustainable within Asian legal orders.²⁸

3 Corporate Accountability in Personal Data Protection in Selected Asian Countries

Methodologically, this section adopts a functional comparative approach to examine how selected ASEAN jurisdictions respond to a common regulatory problem: the domestic translation of trade-linked and market-driven accountability pressures into personal data protection law. Singapore, Thailand, Malaysia, and Vietnam are chosen because they are deeply integrated into regional and global value chains, yet differ in legislative maturity, regulatory capacity, enforcement style, and patterns of state-market coordination.

Unlike the European model, which places personal data protection within the framework of fundamental individual rights, several Asian countries such as Singapore, Thailand, and Malaysia are developing accountability in a manner closely associated with developmental governance. Accordingly, corporate accountability entails implementing, explaining, and demonstrating compliance with data protection obligations, while also

serving as an intermediary mechanism for balancing privacy protection with digital economic development, while maintaining state oversight over the use and protection of personal data held or controlled by enterprises. As aforementioned, “labour data” refers to personal data associated with recruitment, the course of employment, and termination of the employment relationship; its protection is examined within the legal framework for personal data protection. The four jurisdictions are compared by reference to the specificity of duties to protect data and demonstrate compliance; requirements concerning internal policies, personnel, and governance procedures; and mechanisms of supervision, sanctions, and enforcement practice. The analysis draws on the legal provisions and reported cases, distinguishing regulatory design from enforcement outcomes.

Voluntary instruments retain considerable importance in Asia, reflected by the application of principal soft-law foundation as the National Action Plans implementing the UN mandatory, UN’s SDG disclosure, the GRI framework, etc.²⁹ However, the enforcement and compliance present persistent weaknesses. The legal issues in domestic jurisdictions can be raised from the absence of law on investors’ social accountability in investment treaties, highlighting regulatory chill as a structural feature whereby broad interpretation of the principle of “fair and equitable treatment” by investment tribunals undermine states’ capacity to implement protective measures.³⁰ Besides, enforcement in the criminal law of some states remains focused on individual offenders and unpopularity addresses systemic organizations fault.

The digital economy intersects with corporate accountability and trade law across several distinct vectors in domestic jurisdiction: the regulation of cross-border e-commerce, the governance of AI and algorithmic systems, data sovereignty and cross-border data flows, and

²⁹ UN Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework UN Doc A/HRC/17/31 (21 March 2011); Global Reporting Initiative, GRI Standards; OECD, OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD 2023)

³⁰ Garimella SR, Rajsingh S (2024), “Bilateral investment treaties and investors’ social accountability: the law and praxis in South Asia”. *Journal of International Trade Law and Policy*, Vol. 23 No. 2-3 pp. 129-153, doi: <https://doi.org/10.1108/JITLP-04-2024-0025>

²⁸ *Id.*, 24, 25

the use of digital technologies to enhance compliance and transparency.³¹

3.1 Singapore

Singapore has an economy that is heavily dependent on trade, financial services, digital technology, and global data flows. Consequently, the city-state has needed to establish a sufficiently reliable legal environment to attract international investment, promote electronic commerce, and participate deeply in global digital supply chains.³² In this context, accountability requirements are intended to satisfy international standards on data governance embodied in free trade agreements, cross-border data cooperation mechanisms, and international norms. The EU-Singapore Free Trade Agreement (EU-SFTA) contains a separate chapter on Trade and Sustainable Development (TSD), including strong commitments relating to sustainability and labour issues, such as the protection of labour rights and the environment. The Court of Justice of the European Union (CJEU) has previously ruled, in cases concerning the EU-Singapore Free Trade Agreement, that certain provisions in free trade agreements may render such agreements “mixed agreements” under EU law. The incorporation of Corporate Social Responsibility (CSR) provisions may have a similar effect, altering the commercial nature of free trade agreements and requiring ratification under both EU and national procedures.³³ As Singapore integrates responsible business practices into international trade, including corporate accountability obligations, the legal and practical issues surrounding mixed agreements and the nature of free trade agreements are likely to continue being interpreted in different ways. At the same time, with its ambition to become a trusted hub for data-driven businesses in the Asia-Pacific region,

Singapore must establish mechanisms that require enterprises to demonstrate that data processing activities are conducted in a secure, transparent, and accountable manner in order to maintain the confidence of investors, international partners, and consumers within the digital economy.

In terms of the specification of obligations and guidance on organizing compliance, Singapore illustrates the “accountability-based data governance” model. According to the Personal Data Protection Commission (PDPC), accountability is a foundational principle of the Personal Data Protection Act (PDPA), under which organizations are responsible for the personal data under their management and must also be able to demonstrate compliance with data protection obligations. Part VI of the Singapore PDPA sets out the core obligations of organizations in the care and management of personal data. Accordingly, Sections 23 to 26 require organizations to make reasonable efforts to ensure that collected personal data is accurate and complete, particularly where such data is used to make decisions affecting individuals or is disclosed to another organization. At the same time, organizations are responsible for implementing appropriate security measures to protect personal data against risks such as unauthorized access, collection, use, disclosure, copying, modification, or disposal, as well as to prevent the loss of devices or storage media containing personal data. Singaporean law also requires organizations to cease retaining personal data or to remove how individuals can be identified from such data once the purpose of collection no longer exists and retention is no longer necessary for legal or business purposes. In addition, transfers of personal data outside Singapore may only be carried out where requirements ensuring a standard of data protection comparable to that under the PDPA are satisfied. The Personal Data Protection Commission (PDPC) is empowered to exempt certain requirements relating to data transfer activities on a case-by-case basis, subject to conditions imposed by the Commission, which may be amended or revoked at any time.

When applied to employment relationships, these obligations require enterprises to take steps to maintain the accuracy and security of personnel files, attendance records, and employee assessments, including when such data inform algorithmic management systems. This helps limit adverse decisions based on inaccurate data and unauthorized disclosure of employee infor-

³¹ Mira Burri and Kholofelo Kugler, ‘Regulatory Autonomy in Digital Trade Agreements’ (2024) 27(3) *Journal of International Economic Law* 397-423; Antonio Aloisi, ‘Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-discrimination and Collective Rights’ (2024) 40(1) *International Journal of Comparative Labour Law and Industrial Relations* 37-70.

³² World Trade Organization, *Trade Policy Review: Singapore* (WTO, latest edition).

³³ P M Vu, N H A Vu and C G Nguyen, “Incorporating Corporate Social Responsibility in Free Trade Agreements and Its Impacts on the Multilateral Trade System” in R Roberta (ed), *Repenser les frontières économiques: Le régionalisme est-il une voie prometteuse pour relever les défis globaux?* (TESEO Press 2025) <https://doi.org/10.55778/ts917723237>.

mation. For workplace cameras, the exception allowing processing without consent for managing the employment relationship applies only where the processing is reasonable; enterprises must still notify workers of the purposes of surveillance.³⁴

On 15 July 2019, the Personal Data Protection Commission (PDPC) issued the “Guide to Accountability under the Personal Data Protection Act”, which explains the principle of accountability in the context of personal data protection and how an organization may demonstrate accountability for the personal data under its management. According to the Guide, accountability in relation to personal data protection refers to committing to and demonstrating responsibility for the personal data that an organization holds or controls. Accountability is a fundamental principle of the PDPA, requiring organizations to ensure and demonstrate compliance with the PDPA. Taken together, Sections 11 and 12 of the PDPA constitute the accountability obligation under the PDPA. Although the PDPA imposes mandatory accountability requirements, organizations should consider accountability measures that go beyond mere legal compliance.

According to the Guide, as a matter of good practice, an organization may consider demonstrating accountability in three areas.³⁵

Firstly, regarding policies, in order to ensure a commitment to accountability, it is essential to integrate personal data protection into corporate governance, as the involvement of senior management is crucial. Other accountability measures may include the development and clear communication of personal data protection policies to both internal and external stakeholders. In order to clarify for internal stakeholders their responsibilities and procedures for handling personal data in day-to-day operations, dedicated internal policies should be established.

Secondly, with regard to personnel involved in personal data processing, a structured training and communication plan is essential to equip employees with the necessary knowledge and resources to manage personal data effectively.

Employees involved in handling personal data, as well as those with additional responsibilities, such as designated Data Protection Officers (DPOs), should receive specialized training tailored to their respective areas of responsibility. It is also important that personal data protection policies and procedures be clearly documented and made easily accessible for employees’ reference (for example, through the organization’s intranet).

Thirdly, regarding processes, an accountable organization should establish effective procedures to operationalize its data protection policies throughout the entire data lifecycle (i.e., from the collection to the deletion of personal data) and across all business processes, systems, products, and services. For example, an organization may implement a data protection management programme to operationalize its data protection policies, while also considering the establishment of procedures for conducting Data Protection Impact Assessments (DPIAs) in order to identify and address personal data protection risks. Organizations should regularly review their procedures to ensure that they continue to meet business needs and remain updated in line with regulatory requirements and technological developments.

In enforcement practice, the Personal Data Protection Commission (PDPC) has indicated that, where a data incident occurs, organizations with robust accountability systems may be considered for the application of an “undertaking” mechanism or an “expedited decision” process instead of a full-scale investigation. This demonstrates that Singapore encourages a proactive and cooperative model of data governance between the State and enterprises. In one case involving an educational technology company, the organization had failed to appoint a Data Protection Officer (DPO) for more than five years after its establishment. This omission did not reflect a technical failure, but rather a lack of internal prioritization and accountability, which is precisely the type of outcome that Singapore’s legal framework is designed to prevent. Notably, the organization also argued that the Personal Data Protection Commission should only consider affected individuals located in Singapore when assessing the organization’s data breach, since individuals located overseas would fall within the jurisdiction of foreign regulatory authorities. This argument was rejected by the Commission, which affirmed that organizations operating from Singapore remain accountable for all personal data in their possession or under their control, regardless of where the individuals are

³⁴ Personal Data Protection Commission Singapore, Advisory Guidelines on Key Concepts in the PDPA, ch 16, paras 16.1–16.3; Advisory Guidelines on the PDPA for Selected Topics (revised May 2024), paras 4.39–4.40.

³⁵ Allen & Gledhill, “PDPC Publishes New Guide to Accountability under the Personal Data Protection Act: Demonstrating Accountability for Personal Data” (30 July 2019).

located.³⁶ Under the amendments enacted in 2020 and effective from January 2021, organizations are required to notify the PDPC of any data breach that results in significant harm to affected individuals or is of a significant scale (i.e., involving the personal data of 500 or more individuals). Affected individuals must also be notified where the data breach is likely to result in significant harm to them. The amendments further increased the maximum financial penalty that may be imposed on companies for data breaches to up to 10% of their annual turnover in Singapore or 1 million Singapore dollars, whichever is higher. Prior to these amendments, the maximum penalty for a data breach was capped at 1 million Singapore dollars.³⁷

The educational technology case illustrates obligations to organize compliance internally; the cited account does not identify workers as an affected group. Its relevance to personnel management lies in assigning responsibility for data protection and incident response in relation to employee records. The case does not, however, establish the effectiveness of worker protection in practice.

3.2 Thailand

Thailand is a country that is actively promoting digital transformation and international economic integration through the Thailand 4.0 strategy. The expansion of electronic commerce, digital finance, digital tourism, and high-technology investment has led Thailand to participate increasingly deeply in cross-border data processing and transfer activities.³⁸ This development has created pressure to establish a data protection legal framework that is more compatible with international standards in order to avoid legal risks in international trade and enhance the competitiveness of Thai enterprises within global supply chains. Thailand is also a country facing systemic challenges relating to labour rights. Both Thai workers and migrant workers remain vulnerable to exploitation, retaliation against trade union leaders, systematic underpayment, and the expansion of preca-

rious informal employment.³⁹ Local communities continue to suffer harm arising from land appropriation and environmental degradation, while environmental rights defenders face legal harassment and Strategic Lawsuits Against Public Participation (SLAPPs).

During negotiations on the EU–Thailand Free Trade Agreement (FTA), 20 non-governmental organizations in Thailand jointly submitted a letter to leaders of the European Commission requesting that accountability and human rights protection be ensured throughout the negotiation process of the free trade agreement with the Thai government. These organizations recommended that the European Union adopt several measures to ensure accountability and the protection of human rights.⁴⁰ These recommendations included a proposal to develop a roadmap for ratifying Conventions No. 87 and No. 98 of the International Labour Organization (ILO), to protect freedom of association and collective bargaining. The EU–Thailand FTA remains under negotiation following the resumption of talks in March 2023; proposals on Trade and Sustainable Development (TSD) reflect negotiating objectives and expectations of reform, rather than treaty obligations already in force.⁴¹

With regard to personal data protection, Thailand enacted the Personal Data Protection Act (PDPA) under a framework that is significantly influenced by the GDPR, particularly in relation to legal bases for data processing, data subject rights, sensitive data, cross-border data transfers, and the obligations of data controllers. In terms of the combination of privacy protection and the governance of data processing activities, the Thai approach may be described as a “regulatory hybrid”, namely the combination of privacy protection standards with the practical operational needs of a developing digital economy. Obligations under the Thai PDPA apply to organizations that collect, use, or disclose personal data in Thailand or personal data of Thai residents, including in certain cases where the organization does not have a physical presence in Thailand.

³⁶ Mondaq, “Singapore: A Trusted Hub for Data-Driven Businesses” (21 January 2026).

³⁷ Section 48J of Singapore’s Personal Data Protection Act 2012 (PDPA)

³⁸ Personal Data Protection Act BE 2562 (2019) (Thailand); Notification of the Personal Data Protection Committee on the Protection of Personal Data Sent or Transferred to a Foreign Country (effective 24 March 2024)

³⁹ International Trade Union Confederation, *Global Rights Index* (latest Thailand entry); International Labour Organization materials on labour conditions in Thailand.

⁴⁰ Thai Lawyers for Human Rights, “Thai Civil Society’s Open Letter to the European Commission Ahead of the Next Round of FTA Negotiations: Trade Must Advance, not Undermine, Human Rights” (27 September 2025).

⁴¹ European Commission, EU Trade Relations with Thailand; EU–Thailand Agreement (negotiating status and objectives; accessed 8 October 2026).

Within this framework, corporate accountability is reflected in the requirement that enterprises must demonstrate that data processing activities are based on lawful grounds, carried out transparently toward data subjects, ensure data security, and maintain control over cross-border data transfers. In particular, the new regulations on cross-border data transfers, which came into effect on 24 March 2024, further clarified the mechanisms for relying on appropriate protection standards, including adequacy mechanisms, standard contractual clauses, and binding corporate rules.⁴² An important signal emerging from this wave of enforcement is the willingness of the Personal Data Protection Committee (PDPC) to treat the PDPA as an operational governance framework, encompassing security controls, vendor oversight, and incident response measures, rather than merely a documentation exercise focused on privacy notices and consent forms. In several cases, the PDPC has imposed penalties on both data controllers and data processors involved in processing activities, further reinforcing that accountability under the PDPA is not limited solely to the most visible brand within the processing chain.⁴³ This demonstrates that Thailand is not simply replicating the European privacy model, but is localizing accountability within the broader context of promoting the digital economy, cloud services, electronic commerce, and cross-border investment. The State continues to play a central role through the issuance of standards, the determination of conditions for data transfers, the supervision of compliance, and the imposition of sanctions for violations. Accordingly, accountability in Thailand may be understood as a mechanism for reconciling two objectives: protecting data subjects and minimizing legal risks for enterprises in the process of regional data integration.

For employee data, Section 24 of the PDPA allows processing on grounds of necessity for contractual performance or compliance with a legal obligation. Enterprises must still limit collection and notify the purposes of processing under Sections 22–23; health data, biometric data, and trade union membership data must also satisfy Section 26 on explicit consent or statutory exceptions.⁴⁴ Attendance monitoring and personnel

records management therefore need to be linked to a specific legal basis for processing, enabling workers to understand how their data is used and limiting surveillance beyond legitimate management needs.

The cited Thai cases show that the Personal Data Protection Committee (PDPC) has addressed specific shortcomings in security, processor oversight, and the organization of compliance. The PDPC has issued numerous administrative sanctions totaling more than 21.5 million baht, illustrating the use of administrative sanctions against data-processing organizations. Enforcement cases indicate that the regulatory authority does not merely examine isolated incidents of data leakage, but also evaluates the overall data governance capacity, level of risk control, and internal compliance mechanisms of enterprises. Within the public sector, a state agency providing online services through a system developed by a private enterprise suffered a cyberattack that exposed the personal data of more than 200,000 citizens, with the data subsequently being offered for sale on the dark web. The agency was sanctioned for failing to implement appropriate security measures, failing to conduct risk assessments, and using weak passwords. At the same time, the company responsible for developing the system, acting as a data processor, was also subject to corresponding penalties. In the healthcare sector, a major private hospital was fined more than 1.2 million baht for failing to adequately supervise a document destruction contractor, resulting in the leakage of more than 1,000 medical records containing sensitive health data of patients. Cases in the retail and electronic commerce sectors likewise illustrate the application of accountability obligations. A company engaged in the sale of computers and electronic devices was fined up to 7 million baht for simultaneously violating obligations relating to data security, failing to notify the PDPC of a data breach, and failing to appoint a Data Protection Officer (DPO) despite processing large volumes of personal data. Similarly, a cosmetics company was sanctioned for failing to implement appropriate security measures and failing to comply with data breach notification obligations, while a collectible toy retailer and its associated data processor were also sanctioned for failing to ensure data security. These cases provide evidence of enforcement in relation to security, processor

⁴² Tilleke & Gibbins, “Thailand’s Regulations for Cross-Border Personal Data Transfer Come into Force” (27 March 2024).

⁴³ Chandler Mori Hamada Limited, “Data Protection & Privacy 2026 – Thailand: Trends and Developments” (Chambers and Partners 2026).

⁴⁴ Thailand, Personal Data Protection Act BE 2562 (2019), ss

22–24, 26 and 27; English translation published by Thailand’s Department of Lands.

oversight, DPO appointment, and breach notification obligations.⁴⁵

These cases primarily concern customer, patient, or service-user data and therefore illustrate the enforcement of security, processor management, and breach notification obligations. Applying Sections 37 and 40 of the PDPA to employment, enterprises must specify data protection obligations in agreements with outsourced processors, such as payroll providers, to limit the risk of employee records being disclosed.⁴⁶ These cases are not direct evidence of worker protection against workplace surveillance.

The PDPA, enacted on 28 May 2019, establishes a framework of personal data protection obligations in Thailand; the cited enforcement cases illustrate the application of some of those obligations. The number of cases and the size of penalties are insufficient to establish the effectiveness of protection across the system. Such an assessment requires further evidence of compliance, repeat violations, and redress for harm suffered by data subjects.

3.3 Malaysia

As an important manufacturing, digital services, and electronic commerce hub in Southeast Asia, Malaysia faces pressure to establish a legal environment capable of ensuring data security for international businesses, particularly in the fields of finance, technology, logistics, and cross-border services. The EU–Malaysia FTA remains under negotiation following the resumption of talks in January 2025. Strong and enforceable provisions on Trade and Sustainable Development (TSD), including the protection of workers’ rights, are EU negotiating objectives. Expectations of reform and market pressures on enterprises must therefore be distinguished from TSD obligations under a treaty in force; this FTA has not yet created such obligations.⁴⁷

Malaysia enacted the Personal Data Protection Act in 2010, placing data protection obligations on “data users”. The amendments introduced under the Laws of Malaysia Act A1727 Personal Data Protection (Amendment) Act 2024 introduced provisions on Data Protection Officers (DPOs) in Section 12A and data breach notification in Section 12B. These are specific changes concerning personnel responsible for compliance and incident response procedures. The amending legislation replaced the term “data user” with “data controller”, reflecting a closer alignment with international legal terminology relating to data control.⁴⁸

Another amendment concerns the mechanism for transferring personal data abroad under Section 129 of the PDPA. This change should be assessed by reference to transfer conditions and controller responsibilities, rather than being taken to establish stricter protection or compliance with all international standards.⁴⁹ With these measures in place, and subject to further necessary developments concerning government access to personal data and effective legal remedies, foreign companies may regard Malaysia as a more attractive destination for data-related operations, including data centres and regional operational hubs. Transfer conditions seek to maintain protection when data is processed abroad; their impact on actual data security and consumer confidence depends on compliance, supervision, and remedies for violations.

Finally, by adopting standards similar to those under the GDPR, Malaysia may improve its prospects of being recognized by the European Union as a jurisdiction providing an adequate level of data protection. If recognized under the EU adequacy framework, personal data could flow freely between Malaysia and the European Union without the need for additional safeguards, thereby significantly reducing compliance burdens for businesses that are already engaged in, or seriously considering, international data transfers. These benefits nevertheless remain expectations concerning the impact of reform. The cited material does not provide comparative indicators or enforcement data sufficient to establish the effectiveness of protection, Malaysia’s

⁴⁵ Chandler Mori Hamada Limited, Data Protection & Privacy 2026 – Thailand: Trends and Developments (Chambers and Partners 2026), “Enforcement in 2025”, cases 1–5.

⁴⁶ Thailand, Personal Data Protection Act BE 2562 (2019), ss 37 and 40, on security, breach notification, and controller and processor responsibilities.

⁴⁷ European Commission, EU Trade Relations with Malaysia; EU–Malaysia Agreement (negotiating status and objectives; accessed 8 October 2026).

⁴⁸ Malaysia, Personal Data Protection (Amendment) Act 2024 (Act A1727), ss 2 and 6 (inserting ss 12A–12B into the PDPA 2010). Official text (accessed 8 October 2026).

⁴⁹ Malaysia, Personal Data Protection (Amendment) Act 2024 (Act A1727), s 12 (amending s 129 of the PDPA 2010 on transfers of personal data abroad). Official text (accessed 8 October 2026).

global data protection ranking, or the impact on attracting investment.⁵⁰

In terms of instruments for organizing compliance, Singapore has the guidance on policies, personnel, and processes discussed above, while Malaysia's 2024 amendments introduce obligations concerning DPOs and breach notification. Differences in the type of instrument and the timing of adoption are insufficient to determine which system is undergoing a faster transition. In this context, accountability requires enterprises to organize and demonstrate compliance by establishing internal data governance capacity, including risk identification, allocation of responsibilities, management of data processors, incident response mechanisms, and the ability to demonstrate compliance before regulatory authorities.

In employment management, the principles in Sections 6–12 of the PDPA require enterprises to identify lawful purposes, limit processing to necessary data, provide notice of processing, and protect personnel records. Workers may request access to their data and correction of inaccuracies, subject to statutory grounds for refusal.⁵¹ For payroll records, attendance data, or inputs to employee evaluation systems, access controls and data accuracy help limit unauthorized disclosure and adverse decisions based on inaccurate information.

3.4 Vietnam

In Vietnam, corporate accountability should be assessed through data protection obligations under domestic law, while also considering the context of digital economic integration. Through international cooperation frameworks and new-generation free trade agreements, particularly the EU-Vietnam Free Trade Agreement (EVFTA), as well as commitments within ASEAN, APEC, and international privacy standards, Vietnamese enterprises are increasingly required to demonstrate that their personal data processing activities are conducted on a lawful, transparent, secure, and risk-controllable basis. International integration may provide additional incentives to implement data protection obligations, but does not, by itself, establish the comple-

teness of the regulatory framework or the effectiveness of enforcement in Vietnam.

In terms of substantive obligations, Vietnamese law recognizes requirements concerning the processing, security, and governance of personal data. At present, the most important legal foundations include the Personal Data Protection Law 2025, Decree No. 13/2023/ND-CP on Personal Data Protection, together with relevant provisions contained in the Civil Code 2015, the Law on Cybersecurity 2018, the Law on Cyberinformation Security 2015, the Law on Protection of Consumers' Rights 2023, and sector-specific regulations relating to finance, banking, telecommunications, electronic commerce, and information technology. The necessity of enacting the Personal Data Protection Law 2025 clearly identified the objective of harmonization with international standards and regulations on personal data protection. The experiences of the jurisdictions discussed above concerning data protection obligations, the organization of compliance, and enforcement provide points of reference. Many countries have enacted legal instruments on personal data protection, and numerous such regulations apply to Vietnamese organizations and individuals. Therefore, the incorporation of international rules and precedents on personal data protection must ensure harmonization in a manner suitable to the Vietnamese context, while also maintaining legal compatibility to facilitate implementation by both domestic and foreign enterprises and avoid inconsistencies with obligations under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the EU-Vietnam Free Trade Agreement (EVFTA), and the ASEAN-China Free Trade Area (ACFTA). With respect to accountability in personal data protection, existing provisions establish certain duties to organize and demonstrate compliance, including requirements for enterprises to implement personal data protection measures, conduct data processing impact assessments, control cross-border data transfers, manage third-party data processors, and provide notifications in the event of personal data breaches.

Directly relevant to employment, Article 25 of the Personal Data Protection Law 2025 requires enterprises to collect only information serving recruitment purposes, process it with the applicant's consent, and delete or destroy it if the applicant is not recruited, unless otherwise agreed. Employee data must be retained for the period prescribed by law or agreed upon; upon ter-

⁵⁰ IAPP, "Malaysia's PDPA Amendments: Delivering Enhanced Data Governance and Transparency" (19 September 2024).

⁵¹ Malaysia, Personal Data Protection Act 2010 (Act 709), ss 6–12; text published by Malaysia's Personal Data Protection Department.

mination of the employment contract, it must be deleted or destroyed unless the law or an agreement provides otherwise. The use of technology for employee management must be lawful, protect workers' rights and interests, and be based on their clear awareness of the measures applied.⁵² These requirements help limit prolonged retention of personnel records and non-transparent surveillance.

The impact of the EU-Vietnam Free Trade Agreement (EVFTA) on Vietnam has played an important role in shaping accountability along market-oriented and integration-driven lines. Although the EVFTA is not a specialized agreement on personal data protection, it strongly promotes responsible business practices in Vietnam through requirements relating to sustainable development, labour, transparency, compliance, and corporate responsibility within supply chains. The EVFTA not only promotes trade liberalization, but also emphasizes the importance of sustainable development through the adoption of responsible business practices, particularly in labour-intensive sectors such as textiles, footwear, printing, and wood processing.⁵³ From the perspective of personal data protection, this logic carries significant implications: as Vietnamese enterprises participate more deeply in supply chains involving EU partners, corporate responsibility is no longer confined to product quality, labour conditions, or environmental standards, but also extends to data governance and the protection of information relating to employees, customers, suppliers, and business partners. Enterprises seeking to maintain commercial relationships with high-standard markets such as the European Union are therefore required to develop the capacity to demonstrate compliance, including maintaining records of data processing activities, establishing data protection policies, supervising third-party processors, ensuring information security, and responding appropriately to data breaches. In addition, the implementation of commitments under the EVFTA requires not only improvements in national legislation, but also the establishment of "internal control tool within the enterprises", namely internal compliance control mechanisms designed to ensure

practical compliance within business operations.⁵⁴ Accordingly, the EVFTA may be regarded as an indirect driver of corporate accountability in personal data protection in Vietnam by linking personal data protection with responsible business practices and the competitiveness of enterprises within international markets.

Vietnamese enterprises, particularly those operating in the fields of technology, finance, electronic commerce, digital services, or global supply chains, may be required to comply with personal data protection requirements imposed by foreign partners, investors, or cross-border standards. These requirements may create incentives for enterprises, alongside compliance with domestic law, to establish internal data governance mechanisms, privacy policies, incident response procedures, and compliance demonstration mechanisms in order to satisfy accountability requirements within the international business environment.

The obligations concerning recruitment, retention, and processing of employee data under Article 25 of the Personal Data Protection Law 2025, together with the security and governance requirements discussed above, provide a basis for identifying corporate responsibilities at the regulatory level. Assessing enforcement effectiveness requires further evidence of compliance, supervision, and remedies for violations. These provisions alone do not establish that Vietnam's system provides more or less effective protection than the other jurisdictions compared.

4 Conclusion

This article argued that corporate accountability for labor-data protection should be conceptualized as an emerging issue of sustainable trade governance rather than as a matter confined to privacy law. The analysis of the EVFTA and EUSFTA has shown that, although their TSD chapters do not expressly regulate labour data, they nonetheless alter the normative structure of trade by embedding labour protection, non-regression, monitoring, and participatory implementation mecha-

⁵² National Assembly of Vietnam, Law on Personal Data Protection No 91/2025/QH15 (26 June 2025), art 25, on personal data protection in recruitment and employee management.

⁵³ D T Chien, H X Dung and L M Son, "The Impact of the EVFTA on Responsible Business Practices in Vietnam: Implementation and Challenges" (2025) 15(2) *TaTech Journal of European Studies* 108–122, <https://doi.org/10.2478/bjes-2025-0023>.

⁵⁴ L T T Huong, "Towards Enforcement of Labor Standards in the European Union–Vietnam Free Trade Agreement: Can Vietnam Leverage the Impact of the Implementation of Corporate Social Responsibility?" (2025) 15(2) *TaTech Journal of European Studies* 123–139, <https://doi.org/10.2478/bjes-2025-0024>.

nisms within market integration. Read together with the Brussels Effect, these provisions help explain potential channels of influence on domestic data governance. The EU–Thailand and EU–Malaysia negotiations are examined as sources of reform expectations, distinct from treaty obligations in force and from market-driven incentives.

The comparison identifies differences across the four jurisdictions in the specification of data-protection duties, internal compliance arrangements, and mechanisms of supervision and enforcement. Singapore combines statutory obligations with guidance on policies, personnel, and processes; Thailand’s legislation and reported cases illustrate requirements concerning lawful processing, security, and processor oversight; Malaysia’s 2024 amendments introduce specific obligations concerning data protection officers and breach notification; and Vietnam’s framework includes express requirements for recruitment and employee-data management. These arrangements identify responsibilities relevant to personnel records, workplace monitoring, and the use of data in managerial decisions. The differences concern regulatory design and documented enforcement; they do not establish a hierarchy of national maturity or demonstrate that one system protects workers more effectively than another. Cases involving customer or patient data illustrate organisational duties but provide only indirect support for assessing protection in employment relationships.

Based on these comparative findings, the article advances normative proposals at three interconnected levels.

At the treaty level, future EU-Asia trade instruments should address more explicitly the relationship between sustainable trade, digital governance, and labour-data risks, including algorithmic management and workplace surveillance. Cooperation, monitoring, and reviewing mechanisms within TSD chapters could support this engagement without treating existing chapters as sources of direct corporate data-protection obligations.

At the domestic level, reform should focus on clearer allocations of organizational responsibility, stronger impact-assessment duties, more effective processor oversight, reliable breach-response obligations, and accessible remedies for workers adversely affected by harmful data practices. Their practical contribution should be assessed

through evidence of compliance, supervision, and redress, alongside the content of legal rules.

At the enterprise level, labour-data governance should form part of core compliance architecture rather than a peripheral privacy concern. This entails assigning responsibility for employee-data processing, documenting the grounds and safeguards for its use, and enabling workers to obtain explanations and seek remedies. These proposals connect the article’s sustainable trade perspective with identifiable corporate duties, while recognising that effective worker protection depends on their implementation within domestic legal systems.

References

- ABRAHA, Halefom. Regulating algorithmic employment decisions through data protection law. *European Labour Law Journal*, v. 14, n. 2, p. 172–191, 2023.
- ALOISI, Antonio. Regulating algorithmic management at work in the European Union: data protection, non-discrimination and collective rights. *International Journal of Comparative Labour Law and Industrial Relations*, v. 40, n. 1, p. 37–70, 2024.
- ASIAN DEVELOPMENT BANK. *Asian economic integration report 2021: making digital platforms work for Asia and the Pacific*. Manila: Asian Development Bank, 2021.
- BARTELS, Lorand. Human rights and sustainable development obligations in EU free trade agreements. *Legal Issues of Economic Integration*, v. 40, n. 4, p. 297–313, 2013.
- BRADFORD, Anu. *The Brussels effect: how the European Union rules the world*. Oxford: Oxford University Press, 2020.
- BRONCKERS, Marco; GRUNI, Giovanni. Retooling the sustainability standards in EU free trade agreements. *Journal of International Economic Law*, v. 24, n. 1, p. 25–51, 2021.
- BURRI, Mira. Digital trade law and human rights. *AJIL Unbound*, v. 117, p. 110–115, 2023.
- BURRI, Mira; KUGLER, Kholofelo. Regulatory autonomy in digital trade agreements. *Journal of International Economic Law*, v. 27, n. 3, p. 397–423, 2024.

- CARROLL, Archie B. Corporate social responsibility: evolution of a definitional construct. *Business & Society*, v. 38, n. 3, p. 268–295, 1999.
- CHIEN, D. T.; DUNG, H. X.; SON, L. M. The impact of the EVFTA on responsible business practices in Vietnam: implementation and challenges. *TaTech Journal of European Studies*, v. 15, n. 2, p. 108–122, 2025. Available at: <https://doi.org/10.2478/bjes-2025-0023>.
- DE FRANCESCO, Fabrizio; GUASCHINO, Edoardo. Reframing knowledge: a comparison of OECD and World Bank discourse on public governance reform. *Policy and Society*, v. 39, n. 1, p. 113–128, 2020.
- DE STEFANO, Valerio. *Negotiating the algorithm: automation, artificial intelligence and labour protection*. Geneva: International Labour Office, 2018. (Employment Working Paper No. 246).
- EUROPEAN UNION. 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 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, p. 1–88, 2016.
- EUROPEAN UNION; SINGAPORE. *Free trade agreement between the European Union and the Republic of Singapore*. Chapter 12, 2018.
- EUROPEAN UNION; VIET NAM. *Free trade agreement between the European Union and the Socialist Republic of Viet Nam*. Chapter 13, arts. 13.1–13.2, 13.15–13.17, 2019.
- GARIMELLA, S. R.; RAJSINGH, S. Bilateral investment treaties and investors’ social accountability: the law and praxis in South Asia. *Journal of International Trade Law and Policy*, v. 23, n. 2–3, p. 129–153, 2024.
- GLOBAL REPORTING INITIATIVE. *GRI 1: foundation 2021*. Amsterdam: Global Reporting Initiative, 2021. Available at: <https://www.globalreporting.org/publications/documents/english/gri-1-foundation-2021/>.
- GREENLEAF, Graham. *Asian data privacy laws: trade and human rights perspectives*. Oxford: Oxford University Press, 2014.
- HARDING, Andrew; SIDEL, Mark (ed.). *Central and Southeast Asian legal systems*. Cambridge: Cambridge University Press, 2021.
- HARRISON, James. Trade agreements and sustainability: exploring the potential of global value chain (GVC) obligations. *Journal of International Economic Law*, v. 26, n. 2, p. 199–215, 2023.
- HARRISON, James et al. Labour standards provisions in EU free trade agreements: reflections on the European Commission’s reform agenda. *World Trade Review*, v. 18, n. 4, p. 635–657, 2019.
- HUONG, L. T. T. Towards enforcement of labor standards in the European Union–Vietnam Free Trade Agreement: can Vietnam leverage the impact of the implementation of corporate social responsibility? *TaTech Journal of European Studies*, v. 15, n. 2, p. 123–139, 2025. Available at: <https://doi.org/10.2478/bjes-2025-0024>.
- INTERNATIONAL LABOUR OFFICE. *World employment and social outlook 2021: the role of digital labour platforms in transforming the world of work*. Geneva: International Labour Office, 2021.
- INTERNATIONAL LABOUR ORGANIZATION. *Materials on labour conditions in Thailand*. Geneva: International Labour Organization, s.d.
- INTERNATIONAL TRADE UNION CONFEDERATION. *Global rights index*. Brussels: International Trade Union Confederation, s.d.
- MESSENGER, Gregory. Free trade agreements as sites of economic diplomacy: agreeing common standards for sustainable development. *World Trade Review*, v. 24, n. 2, p. 194–213, 2025. Available at: <https://doi.org/10.1017/S1474745624000296>.
- MISHRA, Neha; PALACIO VALENCIA, Ana Maria. Digital services and digital trade in the Asia Pacific: an alternative model for digital integration? *Asia Pacific Law Review*, v. 31, n. 2, p. 489–513, 2023.
- NAVARRA, Cecilia. *Corporate due diligence and corporate accountability*. Brussels: European Parliamentary Research Service, 2020.
- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD guidelines for multinational enterprises on responsible business conduct*. Paris: OECD Publishing, 2023.
- PERSONAL DATA PROTECTION COMMISSION. *Guide to accountability under the Personal Data Protection Act*. Singapore: Personal Data Protection Commission, 15 July 2019.

STEELE, Vasso. Corporate social responsibility, data protection and the right to privacy. *Student Law Journal*, v. 2, p. 23–43, 2022.

TAMVADA, Mallika. Corporate social responsibility and accountability: a new theoretical foundation for regulating CSR. *International Journal of Corporate Social Responsibility*, v. 5, article 1, 2020.

THAILAND. *Personal Data Protection Act B.E. 2562 (2019)*. 2019.

THAILAND. PERSONAL DATA PROTECTION COMMITTEE. *Notification of the Personal Data Protection Committee on the protection of personal data sent or transferred to a foreign country*. Effective 24 March 2024.

UNITED NATIONS. HUMAN RIGHTS COUNCIL. *Guiding principles on business and human rights: implementing the United Nations “Protect, Respect and Remedy” framework*. UN Doc. A/HRC/17/31, 21 March 2011.

VAN DER MERWE, Joanna; AL ACHKAR, Ziad. Data responsibility, corporate social responsibility, and corporate digital responsibility. *Data & Policy*, v. 4, article e12, 2022.

VAN ’T WOUT, Daan. The enforceability of the trade and sustainable development chapters of the European Union’s free trade agreements. *Asia Europe Journal*, v. 20, p. 81–98, 2022.

VELUT, Jean-Baptiste. Trade linkages or disconnects? Labor rights and data privacy in US digital trade policy. *Politics and Governance*, v. 11, n. 1, p. 249–260, 2023.

VU, P. M.; VU, N. H. A.; NGUYEN, C. G. Incorporating corporate social responsibility in free trade agreements and its impacts on the multilateral trade system. In: ROBERTA, R. (ed.). *Repenser les frontières économiques: le régionalisme est-il une voie prometteuse pour relever les défis globaux?* TESEO Press, 2025. Available at: <https://doi.org/10.55778/ts917723237>.

WOODS, Cindy. Engaging the U.N. guiding principles on business and human rights: the inter-American commission on human rights & the extractive sector. *Revista de Direito Internacional*, Brasília, v. 12, n. 2, p. 570–588, 2015. Available at: <https://doi.org/10.5102/rdi.v12i2.3572>.

WORLD TRADE ORGANIZATION. *Trade policy review: Singapore*. Geneva: World Trade Organization, 2021. Available at: https://www.wto.org/english/tratop_e/tpr_e/tp513_crc_e.htm.