NEWSLETTER

NISHIMURA & ASAHI

Vietnam: Key Developments in the Legal Framework Governing Cybersecurity, Artificial Intelligence, and Data Privacy

Asia & Data Protection Newsletter January 19, 2026

Authors:
Tomonobu Murata
to.murata@nishimura.com
Nguyen Tuan Anh
n.t.anh@nishimura.com
Nguyen Thi Thanh Ngoc
n.t.t.ngoc@nishimura.com
Nguyen Dieu Anh
n.d.anh@nishimura.com

Contents

Ⅰ Introduction

Vietnam's digital economy is evolving at an unprecedented pace, driven by rapid adoption of technology and the increasing importance of data to business operations. As organizations embrace cutting-edge technologies like artificial intelligence (AI), cross-border data flows, and management of internal data processing activities, the need for a robust legal framework has become critical. In response, Vietnamese authorities enacted a series of landmark laws and regulations on an urgent basis in late 2025, to shape the future of cybersecurity, AI, and data privacy in the country. These include:

(i) Law No. 116/2025/QH15 of the National Assembly dated December 10, 2025, on Cybersecurity ("**2025 Cybersecurity Law**");

(ii) Law No. 134/2025/QH15 of the National Assembly dated December 10, 2025, on Artificial Intelligence ("**AI Law**"); and

(iii) Decree No. 356/2025/ND-CP of the Government dated December 31, 2025 ("**Decree 356**"), which details a number of articles and measures for implementation of the Law on Personal Data Protection.[1]

This newsletter outlines key regulations in the new laws, to help businesses understand and meet their obligations on a proactive basis, as several of these regulations entered into effect in January 2026.

[1] Law No. 91/2025/QH15 of the National Assembly dated June 26, 2025, on Personal Data Protection ("**Law on Personal Data Protection**"). For more information, please see our newsletter on this important topic: Vietnam's New Privacy Law: Key Regulations and A Comparative Analysis of Existing Frameworks | N&A Newsletters | Knowledge | Nishimura & Asahi.

II The Big Picture: Why These Laws Matter?

The recent legislative overhaul of technology and data protection law in Vietnam is a strategic move, to position the country as a secure and competitive digital hub in Southeast Asia. Understanding the rationale behind these laws will help businesses appreciate their importance and prepare for compliance in an effective manner.

As e-commerce, fintech, cloud computing, and AI-driven services are growing rapidly and creating vast amounts of personal data, Vietnam is establishing a more robust legal framework for personal data protection through Decree 356 to safeguard personal data, ensuring security, trust, and accountability in the digital environment.

Cyber threats are escalating globally, and Vietnam is no exception. Data breaches, ransomware attacks, and online fraud have become more sophisticated, targeting both individuals and corporations. A series of major cybersecurity incidents over the past two years, ranging from the cyberattacks on VNDirect's securities trading system and PV OIL's information systems in early 2024 to the data breach that exposed Vietnam Airlines' customer information in late 2025, has served as a stark wake-up call for Vietnamese businesses and regulatory authorities.[2] The 2025 Cybersecurity Law was introduced as a responsive legislative measure, to monitor and mitigate these risks.

AI is revolutionizing various industries in Vietnam, from healthcare and finance to retail and logistics. The government also has prioritized AI as a key driver of its National Digital Transformation Program, with the goal of making Vietnam a regional leader in AI innovation by 2030. However, rapid adoption without adequate oversight poses significant risks, as unchecked AI development can lead to bias, misuse, and ethical issues. Therefore, the AI Law was enacted to establish a framework that strikes a balance between fostering AI development and managing associated risks.

Given the current state of the digital economy, virtually all businesses in Vietnam will fall within the scope of these new laws and regulations. Companies that prepare for compliance in advance will secure competitive advantages, strengthen customer trust, and mitigate operational risks. Conversely, noncompliance may result in severe sanctions, reputational damage, and even suspension of business operations.

III In Focus: Notable Requirements

3.1. Cybersecurity Regulations

Overview

The 2025 Cybersecurity Law will take effect on July 1, 2026 and represents a significant upgrade to Vietnam's current legal framework for cybersecurity, by consolidating and unifying the 2018 Cybersecurity Law[3] with the

[2] For more details, please see: for the Vietnam Airlines cybersecurity incident: Vietnam Airlines | Information Regarding Customer Data Breach, for the PVOIL cybersecurity incident: PRESS RELEASE Regarding the Restoration of PVOIL's Information Technology System - PVOIL, and for the VNDirect cybersecurity incident: VNDirect cyberattack causes big splash on stock market.

[3] Law No. 24/2018/QH14 of the National Assembly dated June 12, 2018, on Cybersecurity.

2015 Cyber Information Safety Law[4] and introducing stricter requirements to address growing cyber threats and protect national security in the digital age.

Extraterritorial application

The 2025 Cybersecurity Law extends its scope of applicability, to include offshore agencies, organizations, and individuals directly engaging in or related to the activities of cybersecurity protection, as well as trading in cybersecurity products and services in Vietnam.[5]

Key requirements for ensuring cyber-information security

All enterprises, including offshore enterprises, that provide services via telecommunications networks and the internet, as well as value-added services on cyberspace in Vietnam (collectively "**Covered Enterprises**"), are subject to numerous obligations and requirements, notably including:

(i) Verification of user information

The 2025 Cybersecurity Law merely requires Covered Enterprises to verify information when a user registers for a digital account, without providing additional details on the type of information to be verified or the verification method.[6]

(ii) Collaboration with the authorities to handle cybersecurity noncompliance

To facilitate the verification, investigation, and handling of violations of cybersecurity laws, upon receipt of a request from the specialized cybersecurity agency of the Ministry of Public Security ("**MPS**") by various means (e.g., verified emails or phone calls), Covered Enterprises may be obligated to perform the following processes, depending on the specific content of the request:

(a) provide users' information to the specialized cybersecurity agency of the MPS within 24 hours (or 3 hours in emergency situations that threaten national security or endanger human lives);[7] and/or

(b) prevent the sharing of information, delete information, or remove services and applications containing content that violates the 2025 Cybersecurity Law within 24 hours (or 6 hours in emergency situations that threaten national security or endanger human lives), and store the

[4] Law No. 86/2015/QH13 of the National Assembly dated November 19, 2015, on Cyber Information Safety (as amended).

[5] 2025 Cybersecurity Law, Article 1.2.(c).

[6] 2025 Cybersecurity Law, Article 25.2.(a).

[7] 2025 Cybersecurity Law, Article 25.2.(a).

relevant system logs.[8]

(iii) Data storage requirements

Covered Enterprises must store service users' personal information and data generated by users, including: account names, service usage time, service fee payment information, IP addresses used to access relevant services, and other related data, for the period prescribed by law, after the user has finished using the service.[9] The method and location of storage required to comply with this obligation is unclear, and not set forth in the 2025 Cybersecurity Law. Relevant details may be clarified in the government's guiding decree, which may be released soon.

(iv) Data localization requirement

Covered Enterprises that collect, exploit, analyze, and process data relating to personal information, data on the relationships of service users, and data created by service users in Vietnam must implement and use the data protection measures prescribed by law and store the data in Vietnam for the period required by the government.[10] Covered Enterprises that are offshore enterprises must establish a branch or representative office in Vietnam for this purpose.[11] The data localization requirement in the 2025 Cybersecurity Law largely mirrors the framework established in the 2018 Cybersecurity Law. However, variations may arise depending on the specific provisions set forth in the forthcoming government decree that will provide detailed guidance on this requirement.

3.2. AI Regulations

Overview

Initially, AI issues were to be governed by the Law on Digital Technology Industry and its guiding regulations.[12] However, in a swift and decisive legislative shift, Vietnamese lawmakers enacted a comprehensive standalone statute, the AI Law, which is the country's first dedicated legal framework governing AI and underscores the fact that AI development currently is one of the country's top priorities. The AI Law was adopted by the National Assembly on December 10, 2025, and will take effect on March 1, 2026, with the primary objectives of promoting responsible AI innovation, safeguarding ethical standards, and managing risks associated with AI.

8 2025 Cybersecurity Law, Article 25.2.(b).

9 2025 Cybersecurity Law, Article 25.2.(d).

10 2025 Cybersecurity Law, Article 25.3.

11 2025 Cybersecurity Law, Article 25.3.

12 Law No. 71/2025/QH15 of the National Assembly dated June 14, 2025, on the Digital Technology Industry, Chapter IV. For more information about this law, please see our previous newsletter: Vietnam: Official Introduction of Vietnam's First AI Act | N&A Newsletters | Knowledge | Nishimura & Asahi

Scope of Applicability

The AI Law governs all activities relating to AI on a comprehensive basis, including research, development, provision, deployment, and use of AI systems by Vietnamese agencies, organizations, and individuals, as well as foreign organizations and individuals.[13] Notably, AI activities that serve only the purposes of Vietnam's national defense, security, and ciphers are not subject to the AI Law.[14]

Concepts: AI, AI Systems

The AI Law defines AI as the electronic implementation of human intellectual capabilities, including learning, reasoning, perception, judgment, and understanding natural language.[15] Another key concept set forth in the AI Law is "AI system," which is defined as a machine-based system designed to perform AI capabilities with varying degrees of autonomy, capable of self-adaptation after deployment, where the system makes inferences from input data, based on clearly defined or implicitly formed objectives, to produce outputs such as predictions, content, recommendations, or decisions that can influence the physical or digital environment.[16] These two foundational definitions establish the scope of governance of the AI Law and serve as the basis for application of its regulatory requirements.

AI Stakeholders

The AI Law separates AI stakeholders into the following five major groups, and imposes relevant regulations based on a given stakeholder's classification:

(i) AI developer: an organization or individual that designs, builds, trains, tests, or refines all or part of an AI model, algorithm, or system, and has direct control over the technical methodology, training data, or model parameters.[17]

(ii) AI provider: an organization or individual that brings AI systems to market or puts them into use under its own name, brand, or trademark, whether the system was developed by the provider or by a third party.[18]

(iii) AI deployer: an organization or individual that uses AI systems under its control in professional or commercial activities, or in the provision of services, excluding situations in which the system is used

13 AI Law, Articles 1.1 and 2.

14 AI Law, Article 1.2.

15 AI Law, Article 3.1.

16 AI Law, Article 3.2.

17 AI Law, Article 3.3.

18 AI Law, Article 3.4.

for personal or non-commercial purposes.[19]

(iv) AI user: an organization or individual who interacts directly with AI systems or uses the output of those systems.[20]

(v) AI-impacted entity: an organization or individual whose legal rights, interests, life, health, property, reputation, or access to services is impacted directly or indirectly by the deployment or output of AI systems.[21]

Incentives and Support for AI Development

Organizations and individuals operating in the field of AI are entitled to the highest levels of incentives and support set forth in the laws on science and technology, investment, digital technology industry, high technology, digital transformation, and related laws, and also receive facilitated access to infrastructure, data, and testing environments serving research, production, and commercialization of AI products and services.[22]

A national AI development fund was introduced pursuant to the AI Law, with a unique financial mechanism that accepts risks in science, technology, and innovation, allocates capital flexibly based on progress and implementation requirements without depending on the fiscal year, and applies simplified procedures for strategic tasks or those requiring rapid implementation.[23] The fund prioritizes investment, financing, and support for the development of AI infrastructure, research, development, and master core AI technologies, and developing AI enterprises, among other stated priorities.[24]

Risk-based Classification of AI Systems

The AI Law classifies AI systems into the following three categories for management purposes, based on the risk level of the relevant system:

(i) High risk: AI systems that can cause significant harm to the lives, health, legitimate rights, and interests of organizations and individuals, national interests, public interests, and national security.[25] High-risk AI systems are inspected periodically or when signs of legal violations are discovered.[26]

---

19 AI Law, Article 3.5.

20 AI Law, Article 3.6.

21 AI Law, Article 3.7.

22 AI Law, Article 20.1.

23 AI Law, Article 22.3.

24 AI Law, Article 22.3.

25 AI Law, Article 9.1.(a).

26 AI Law, Article 10.5.(a).

(ii) Medium risk: AI systems that have the potential to confuse, influence, or manipulate users because the users are unable to perceive that the entity with which they are interacting is an AI system or the content that such a system generates.[27] Medium-risk AI systems are monitored through reporting, sample testing, or evaluations by independent organizations.[28]

(iii) Low risk: AI systems that do not fall within the high risk and medium risk categories in items (i) and (ii) above.[29] Low-risk AI systems are monitored and tested in the event of incidents or feedback, or when security needs to be ensured, without creating unnecessary obligations for organizations or individuals.[30]

The risk classification of AI systems is based on criteria such as the level of impact on human rights, safety, and security, the system's area of use, especially essential areas or those directly related to the public interest, the scope of users, and the scale of the system's influence.[31] The government is tasked with establishing more detailed regulations on the risk classification of AI systems, which are likely to be issued in the near future.[32]

Notably, the provider of the AI system has an obligation to perform the risk classification itself before putting the AI system into use, and if an AI system is self-classified in either medium or high risk category, the AI system provider must notify the Ministry of Science and Technology ("**MST**") of the classification before putting the AI system into use.[33] If the AI system provider is unable to classify its AI system, it may ask the MST to provide guidance on the classification, on the basis of a technical dossier.[34]

Management Requirements for AI Systems Based on Risk Classification

(i) High risk AI systems: Among other requirements, high-risk AI systems must: (a) undergo conformity assessments in accordance with the AI Law before being put into use or when significant changes occur during use, and (b) conform with standards or technical regulations for AI systems in accordance with the law on standards and technical regulations (if any).[35] A list of high-risk AI systems, including a list of AI systems subject to conformity assessments, will be provided by the Prime Minister.[36] Notably, offshore providers of high-risk AI systems in Vietnam must have a contact point in Vietnam; if the AI system is subject to mandatory conformity certification before deployment, the providers must have a

27 AI Law, Article 9.1.(b).

28 AI Law, Article 10.5.(b).

29 AI Law, Article 9.1.(c).

30 AI Law, Article 10.5.(c)

31 AI Law, Article 9.2.

32 AI Law, Article 9.3.

33 AI Law, Articles 10.1 and 10.3.

34 AI Law, Article 10.4.

35 AI Law, Article 13.1.

36 AI Law, Article 13.4.

commercial presence or authorized representative in Vietnam.[37]

(ii) Medium risk and low risk AI systems: Among other requirements, both the AI system providers and the deployers are subject to accountability, and must provide explanations if there is a request from the competent authority.[38]

AI Labeling Requirements

The AI system deployer must ensure that audio, images, and videos created or edited using AI systems to simulate or mimic the appearances and voices of real people, or to recreate real events, are clearly labeled to distinguish them from real content.[39] For products created by AI that are cinematographic, artistic, or creative works, the labeling set forth in this section must be done in a manner appropriate to ensure that it does not hinder the display, performance, or enjoyment of the work.[40] The detailed requirements for AI labeling will be provided by the government.[41]

Obligations When Handling AI Incidents

If a serious AI incident occurs (i.e., an event occurring in the operation of an AI system that causes or is likely to cause significant damage to life, health, human rights, property, cybersecurity, public order, the environment, or disrupts the operation of information systems critical to national security[42]), the developers and providers of the AI system must implement technical measures promptly to rectify, suspend, or recall the system, and simultaneously notify the competent authority of the incident; deployers and users of AI systems must provide timely notice and cooperate with the process of rectifying the AI incident.[43] Though the AI Law does not state whom AI deployers and users must notify and with whom AI deployers and users must cooperate, given the key responsibilities of AI developers and providers, as well as the state authorities handling AI incidents, it is reasonable to interpret that the AI deployers and users must notify and cooperate with AI developers and providers, and the state authorities.

37 AI Law, Article 14.6.

38 AI Law, Article 15.

39 AI Law, Article 11.4.

40 AI Law, Article 11.4.

41 AI Law, Article 11.6.

42 AI Law, Article 3.8.

43 AI Law, Article 12.2.

3.3. Personal Data Protection Regulations

Overview

Vietnam has strengthened its data privacy regime significantly with the enactment of the Law on Personal Data Protection in mid-2025, and then Decree 356 in late 2025, which provides support and comprehensive guidance for implementation. Both instruments took effect on January 1, 2026, to replace and address the shortcomings in their predecessor, Decree 13,[44] and are a decisive step toward aligning Vietnam's personal data protection framework with international standards.

Detailed Procedures for Data Controllers to Comply With Requests for Exercise of Data Subjects' Rights

Decree 356 compels a data controller or data controller-cum-processor to: (i) develop and issue forms and procedures for the exercise of data subjects' rights, in alignment with data processing activities and the responsibilities of relevant departments, and (ii) ensure that data subjects are informed about the procedures for exercising their rights (e.g., by serving written notice on relevant data subjects).[45]

Decree 356 also specifies timeframes for compliance and actions to be taken to comply with data subjects' exercises of their rights.[46] Notably, the timeframes for a data controller to comply with certain requests have been extended significantly, and are more practical compared with those set forth in Decree 356's predecessor, Decree 13, and a time extension mechanism also has been added.[47] For instance, if a data subject makes a request for data deletion, the data controller must respond to the data subject within 2 working days, provide the data subject with all relevant information about the procedure for data deletion, and perform the deletion within 20 days.[48] If the data controller must ask a data processor or third party to perform the deletion, the time period for deletion is extended to 30 days.[49] Depending on the nature and complexity of the request, the time period for performing the deletion may be extended once for up to 20 more days; when this extension of time occurs, the data controller must notify the data subject of the reason for the extension and is responsible for proving that the extension is necessary and reasonable.[50]

Personal Data Transfer Agreements

Decree 356 mandates that parties to personal data transfers (including both domestic and cross-border transfers) enter into a data transfer agreement containing certain statutory content if the transfer falls within one of the three following classifications: (i) personal data transfers consented to by the data subject, (ii) personal data transfers for continued processing in cases of division, separation, merger of agencies, organizations, and

---

44 Decree No. 13/2023/ND-CP of the government dated April 17, 2023, on Personal Data Protection ("**Decree 13**").

45 Decree 356, Article 5.1.

46 Decree 356, Article 5.

47 Decree 356, Article 5.

48 Decree 356, Article 5.4.

49 Decree 356, Article 5.4.

50 Decree 356, Article 5.4.

administrative units, reorganization and conversion of ownership forms of state-owned enterprises, division, separation, merger, consolidation, and termination of operations of units and organizations, and/or the establishment of units and organizations based on the termination of operations of other units and organizations, and (iii) personal data transfers from a data controller or a data controller-cum-processor to a data processor or a third party, for processing personal data in accordance with the law.[51] Of note, in situation (iii), since parties to the processing of personal data are required by law to enter into a data processing agreement,[52] to save cost and time, relevant statutory content about data transfers may be considered to be included in the data processing agreement.

Separate Requirements for Personal Data Protection in Specialized Fields

Decree 356 establishes additional requirements for personal data protection in a number of fields, like banking & finance, big data, AI, metaverse, blockchain, and cloud computing.[53] Notably:

(i) In addition to complying with other relevant requirements, organizations and individuals operating in the fields of banking, finance, and credit information activities (e.g., local banks, branches of foreign banks, finance companies) must: (a) comply with standards and technical regulations on personal data protection, as well as technical regulations governing de-identification and pseudonymization of personal data (to be issued, and applicable, in Vietnam), (b) conduct annual compliance assessments with regard to personal data protection regulations, and (c) record a log of all personal data processing activities.[54]

(ii) In addition to complying with other relevant regulations, organizations and individuals that sign contracts with cloud computing service providers related to personal data processing must: (a) specify certain content in the relevant contracts (i.e., compliance with Vietnamese laws governing personal data protection, provision of information about the department and personnel responsible for personal data protection, and compliance with administrative procedures related to personal data protection as prescribed by law), (b) immediately notify relevant parties of any changes that may affect personal data, (c) clearly determine the flow of personal data processing, the roles of each party involved in the provision of cloud computing services, and their respective responsibilities, and (d) comply with exercises of rights by data subjects.[55]

Personal Data Processing Impact Assessment (DPIA) and Cross-Border Transfer of Personal Data Impact Assessment (CTIA) (formerly known as OTIA under Decree 13)

Decree 356 establishes new forms for DPIA and CTIA reports, and creates many changes to the content of

51 Decree 356, Article 7.1.

52 Law on Personal Data Protection, Article 37.2(a), (b).

53 Decree 356, Articles 8 to 12.

54 Decree 356, Article 8.1.

55 Decree 356, Article 12.2.

impact assessments, compared with the forms established and used pursuant to Decree 13. Decree 356 appears to have restructured impact assessments comprehensively, from a broad assessment of various issues, such as social or economic impact, as required under Decree 13, to a pronounced focus on the risks associated with processing and cross-border transfers of personal data.[56]

Decree 356 also specifies situations in which an update to previously submitted DPIA and CTIA dossiers is required; for clarity, these situations also trigger updates to submitted DPIA and OTIA dossiers during the effective period of Decree 13.[57] The regime for updating previously submitted DPIA and CTIA dossiers is comprised of: (i) a periodic update every 6 months from the date of first submission of the dossier, if there are changes to certain types of information in the dossier (e.g., new purposes of processing and cross border transfer of personal data, or new data processor), and (ii) ad-hoc updates within 10 days if there are changes to certain types of information in the dossier (e.g., changes to business lines, services related to personal data processing provided by the data controller that are declared in the submitted dossiers, or changes to the information about the organization or individuals providing personal data protection services).

Enterprises that submitted the DPIA and OTIA dossiers during the effective period of Decree 13 must update the dossiers using the new forms within 10 days after any changes to the information in the submitted dossiers that require an ad-hoc update under Decree 356; meanwhile, although Decree 356 is silent on the starting point of the 6-month period applicable to the periodic update requirement, it is reasonable to interpret that the starting point is calculated from 1 January 2026 (the effective date of Decree 356 (including the provision on updating the submitted DPIA and CTIA dossiers)).

Although not legally mandated to do so, enterprises that submitted DPIA and OTIA dossiers under Decree 13 are strongly advised to prepare and file new DPIA and CTIA dossiers with the competent authority on a proactive basis, due to the significant differences in impact assessment content covered by the old and new forms. This will help mitigate the risk of failure to comply with update obligations, particularly the ad-hoc update requirement, which imposes a strict 10-day deadline from the date of change but still triggers a full update to comply with the new forms.

Notably, in addition to the exceptions set out in the Law on Personal Data Protection, Decree 356 provides some additional exceptions, which exempt personal data exporters from the cross-border transfer impact assessment requirements, including: (i) press and media activities in accordance with the law, (ii) cross-border transfers of personal data that has been publicly disclosed in accordance with the law, (iii) in emergency situations, where it is essential to provide personal data across borders to protect an individual's life, health, and property safety, (iv) to perform duties or obligations prescribed by law, (v) cross-border transfers of personal data for managing personnel across borders in accordance with labor rules, regulations, and collective labor agreements as prescribed by law, and (vi) provision of personal data across borders for purposes of signing contracts or carrying out procedures related to cross-border transportation, logistics, money transfers, payments, hotel bookings, visa applications, and scholarship applications.[58] Although in practice some of these additional exceptions, together with those in the Law on Personal Data Protection, remain vague and

[56] Decree 356, Articles 18 and 19, Forms No. 09 and 10 of the Annex.

[57] Decree 356, Article 20;

[58] Decree 356, Article 17.3;

challenging in interpretation, they are considered positive improvements compared to Decree 13, and create a more business-friendly data governance policy.

Enterprise Requirements for Data Protection Officers ("DPO") and Data Protection Units ("DPU")

Decree 356 specifies the functions and tasks of DPOs and DPUs, and imposes several competency requirements on DPOs and DPUs.[59] Notably, Decree 356 contains a new requirement (compared with Decree 13) that enterprises sign a confidentiality agreement with their DPOs.[60] Decree 356 does not establish any mandatory content for that confidentiality agreement; however, it provides optional content, which includes exemption from liability in the event of a breach or damage to protected personal data.[61] Decree 356 also requires enterprises to provide their DPOs with training in terms of knowledge and skills relating to personal data protection, but does not contain any details about the nature or content of the training.[62]

IV Conclusion and Recommendations

The recent legislative developments in Vietnam are a decisive shift toward a more structured, accountable, and technologically-aware regulatory environment for data, cybersecurity, and AI. With the introduction of the AI Law, the 2025 Cybersecurity Law, and Decree 356, businesses in Vietnam now face a markedly higher standard of legal compliance. Early assessment, internal gap analysis, and timely implementation of compliance measures, particularly in relation to data governance, cybersecurity safeguards, AI deployment, and incident response, will be critical to mitigating legal and operational risks.

The legal framework will continue to evolve, including through the issuance of a number of guiding regulations and sanctions regulations, practical guidance, and implementation of the law by competent authorities. We recommend that enterprises in Vietnam, and offshore enterprises engaging in relevant data, AI, or cybersecurity activities in Vietnam, monitor these developments closely and engage in ongoing compliance planning. Our firm is committed to supporting businesses through this dynamic period and to providing the insight and guidance necessary to navigate the complexities of, and capitalize on the opportunities presented by, this and other emerging legislation. Please feel free to reach out to us if you have any questions or would like additional assistance.

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com

[59] Decree 356, Articles 13 and 14.

[60] Decree 356, Article 13.5.

[61] Decree 356, Article 13.5.

[62] Decree 356, Article 13.6.