

Special Alert

June 2024

www.indochinecounsel.com

Strengthening Cyber Governance: Vietnam to develop its Draft Decree on Cybersecurity and Data Protection Administrative Violations Sanctions

Recently, the Ministry of Public Security (MPS) has submitted a proposed Draft Decree on Sanctioning Violations in the Cybersecurity Sector (the “**Draft Decree**”), which includes provisions addressing violations related to personal data protection within cyberspace. The Draft Decree consists of 4 Chapters and 51 Articles, structured on various explanatory reports integrating feedback and reviews from the legal framework concerning personal data protection.

Given the significant public interest in the matter at hand, the Draft Decree aims to clarify key issues, such as the subjects of governance, types of violations, and its severity. As a heads-up, this article will offer key insights into the principal provisions of the Draft Decree.

General Provisions

Subject of Application

The Draft Decree extends its scope to both local and foreign entities (organizations and individuals), clearly categorizing them, of which certain notable subjects include:

- (i) Entities established under the Enterprise Law, the Cooperative Law, the Investment Law;
- (ii) Foreign enterprises (or its branches, representative offices, business location) offering telecommunication services, Internet services, cyberspace content provision services, information technology, cybersecurity, and cyber information security;
- (iii) Organizations, enterprises providing internet-based information content services;
- (iv) Organizations, enterprises [involved in] domain name registration;
- (v) Administrators of information systems; and

(vi) Operators of information systems.

From the foregoing, it should be noted that even when a foreign enterprise (or its branches, representative offices, business location) does not fall within the scope of Item (ii) above, they may still be subject to the Draft Decree if being classified as other subjects listed in Article 2.2 thereof.

Although the Draft Decree provides a foundation for improving cyber governance, it presents practical enforcement challenges, particularly towards foreign enterprises without a local commercial presence, due to the legal framework's silence on this matter.

Sanction forms and statute of limitations

Under the Draft Decree, entities (organizations and individuals) found in violation shall face penalties in the form of warnings or fines, along with one or more additional penalties depending on the nature and severity of the violation. Additionally, the entities may be subject to one or more remedial measures to safeguard the legitimate rights and interests of others and support the operations of competent authorities.

The statute of limitations for administrative penalties for all cybersecurity violations is one (1) year, except for violations related to the production, export, import, or trading of cybersecurity products or services, where it will be two (2) years.

Monetary penalties under the Draft Decree apply to violating individuals, which will be doubled towards violating organizations committing the same wrongdoing.

Administrative Violations and Sanctions in Specific Sectors

The Draft Decree specifies violations in five (5) main sectors, including Information Security Assurance; Personal Data Protection; Cyber Attacks Prevention; Cybersecurity Implementation; and Prevention of Using Cyberspace, Information Technology and Electronic Means for Violating Social Order and Safety. Below are some highlights in certain notable fields:

Violations in the field of personal data protection

Violations of data subject's rights

In respect of each data subject's rights under Decree No. 13/2023/ND-CP on personal data protection ("**Decree 13**"), sanctions for violations of the same are set out respectively under Article 14 of the Draft Decree. The fine ranges from VND10 million to VND100 million, accompanied by additional sanctions and remedial measures.

The most severe violation, which is subject to the highest fine in this range, is the act of Data Controller, Data Controller & Processor, Data Processor, and Third Party (if any) preventing data

subjects from lodging complaints, reporting, or initiating legal actions in accordance with and as permitted by applicable laws. Violating entities shall also face revocation of relevant business licenses from one (1) to three (3) months as an additional sanction.

It is worth noting, however, that there are still errors in cross-references to other legislation, particularly in this Article 14 and throughout the Draft Decree in general.

Violations of data subject's consent and unauthorized processing of personal data

Obtaining data subject's consent is one of compulsory conditions for personal data processing under the local laws. Accordingly, the Draft Decree sets out specific sanctions for failure to comply with such obligations of parties engaging in personal data processing. However, the fine range does not seem to be too severe, which is set from VND10 million to a maximum of VND50 million. Additional sanctions as well as remedial measures are also applied, depending on each violation and its severity.

In this regard, the Draft Decree also stipulates significant penalties for unauthorized collecting, transferring, and trading personal data. Violating entities may face fines up to VND100 million, along with additional sanctions and/or remedial measures. Remarkably, for repeated violations, the fine can reach up to five percent (5%) of the violator's total revenue in Vietnam for the preceding fiscal year. This provision proves punitive effect for directly targeting the economic benefit of violators. However, it poses challenges in terms of time and implementation due to difficulties in determining the violator's exact benefit. In addition, violators are also required to make public apology via mass media for their wrongdoings.

Violations of personal data processing notification

According to Article 13.1 of Decree 13, a single notification must be made before initiating any personal data processing activities. Specific violations related to this notification obligation of involved parties have been outlined under Article 17 of the Draft Decree, of which the applicable fine ranges from VND10 million to VND20 million, being accompanied by the remedial measure of forcing the implementation of notification methods for personal data processing towards relevant violations.

Temporary or definite suspension (from one (1) to three (3) months) of personal data processing activities is also mentioned under Article 17, without being assigned as major or additional sanction.

Violations of Personal Data Processing Impact Assessment (PDPIA) and Overseas Personal Data Transfer Impact Assessment (OPDTIA)

To align with the requirements under Decree 13 in terms of PDPIA and OPDTIA, the Draft Decree provides significant sanctions for respective violations, the summary of which is shown in the table below:

Violations	Additional penalties	Remedial measures	Note
For PDPIA			
Fine ranging from VND70 million to VND100 million			
Failing to prepare or maintain records of the PDPIA dossiers: <ul style="list-style-type: none"> by Data Controller, Data Controller & Processor from the commencement of personal data processing; or by Data Processor in performing its contract with Data Controller. 	✓	✓	<ul style="list-style-type: none"> Error is found in Article 25.6(a), regulating remedial measure. Accordingly, the remedial measure under the said Article is quoted as “Force to prepare or not maintain PDPIA dossiers...”, which should not be in negative form; and Violations under Articles 25.2, 25.3 and 25.4 are not assigned with either additional sanctions or remedial measures.
Failing to submit one (1) original of the <i>Notification of PDPIA Dossiers Submission</i> form (Form 04) to A05 attached to the MPS within sixty (60) days from the commencement date of personal data processing.	✓	✓	
Failing to comply with A05’s request to revise or complete the PDPIA dossiers.	✓	✓	
Fine ranging from VND140 million to VND200 million			
Exposing, losing personal data of 100,000 Vietnamese citizens up to under 1,000,000 Vietnamese citizens.	Not mentioned	Not mentioned	
Fine ranging from VND350 million to VND500 million			
Exposing, losing personal data of 1,000,000 Vietnamese citizens up to under 5,000,000 Vietnamese citizens.	Not mentioned	Not mentioned	
Fine equivalent to five percent (5%) of the violator’s total revenue in Vietnam for the preceding fiscal year			
Exposing, losing personal data of 5,000,000 Vietnamese citizens or more.	Not mentioned	Not mentioned	
For OPDTIA			
Fine ranging from VND70 million to VND100 million			
Failing to prepare or maintain OPDTIA dossiers from the commencement of data processing, and to perform regulatory	✓	✓	<ul style="list-style-type: none"> Violations under Articles 26.2, 26.3 and 26.4 are not assigned with either

Violations	Additional penalties	Remedial measures	Note
obligations under Decree 13.			additional sanctions or remedial measures.
Failing to submit one (1) original of the <i>OPDTIA Dossiers</i> to A05 within 60 days from the commencement date of personal data processing.	✓	✓	
Failing to provide A05 with the regulatory information under Article 25.4 of Decree 13 upon successful offshore transfer of personal data.	✓	✓	
Failing to comply with A05's request to revise or complete the <i>OPDTIA</i> dossiers.	✓	✓	
Failing to comply with A05's request for inspection of overseas transfer of personal data.	✓	✓	
<i>Fine ranging from VND140 million to VND200 million</i>			
Exposing, losing, or transferring personal data of 100,000 Vietnamese citizens up to under 1,000,000 Vietnamese citizens overseas.	Not mentioned	Not mentioned	
<i>Fine ranging from VND350 million to VND500 million</i>			
Exposing, losing, or transferring personal data of 1,000,000 Vietnamese citizens up to under 5,000,000 Vietnamese citizens overseas.	Not mentioned	Not mentioned	
<i>Fine equivalent to three percent (3%) to five percent (5%) of the violator's total revenue in Vietnam for the preceding fiscal year</i>			
Exposing, losing, or transferring personal data of 5,000,000 Vietnamese citizens or more overseas.	Not mentioned	Not mentioned	

Violations in Cybersecurity Implementation

Violations of child protection

Protecting children's rights has been receiving continuous attention, particularly in cyberspace where cyberbullying has always been a pressing issue. In conformity with regulations on protecting children

in cyberspace under the Cybersecurity Law 2018 (the “**Cybersecurity Law**”), sanctions for relevant violations of the same have been crafted under the Draft Decree. While failing to prevent the sharing of and deleting harmful/abusing content may face a fine up to VND20 million, actively sharing or dispersing the same will be subject to a fine up to VND50 million. The maximum fine in this field is VND70 million, applicable to those who lack cooperation with authorities in protecting children online, as well as those who encourage children to initiate illegal acts.

Unfortunately, despite being regulated under Decree 13, violations in terms of protecting personal data of children have yet to be addressed under the Draft Decree.

Violations of data storage, establishing branches or representative offices in Vietnam

The requirements for data localization/storage and branches/representative office establishment under the Cybersecurity Law have been raising concerns among relevant entities. Offshore organizations, in particular, are uncertain about whether they need to comply and, if so, when and how to achieve such compliance.

Apart from serving as a legal framework for violations of this requirement, enhancing cyber security compliance, the Draft Decree, in particular Article 38 thereof, has somehow implied that the said requirement is applied to offshore entities on conditions (i.e., fields of operation) and/or upon request by competent authorities.

Article 38 of the Draft Decree sets a fine range from VND70 million to VND100 million for violations related to this matter, all of which are accompanied by additional sanctions as well as remedial measures.

A typo mistake is discovered under Article 38.1(a), quoting the Cybersecurity Law’s guiding decree as “Decree No. 53/2023/ND-CP”, which should be “Decree No. 53/2022/ND-CP” instead.

Conclusion

The proposed Draft Decree is set to take effect from 1 June 2024. Although meeting this timeline appears unlikely given the current status of the Draft Decree, it underscores the pressing need for regulations addressing cybersecurity violations. Despite its broadly defined penalty clauses, the issuance of this Draft Decree is expected to pose significant impact on concerned entities, prompting them to make necessary adjustments to comply with legal obligations, particularly in matters involving foreign entities and personal data protection.

About Indochine Counsel

Established in October 2006, Indochine Counsel is a leading commercial law firm in Vietnam. Our firm is ideally positioned to assist international investors and foreign firms to navigate the legal landscape in one of Asia's most dynamic and challenging countries. We also take pride in our services offered to domestic clients in searching for opportunities abroad. With over 45 lawyers many of whom have been trained abroad and staffs in two offices, Ho Chi Minh City and Hanoi, Indochine Counsel offers expertise in a dozen practice areas and provides assistance throughout the entire life cycle of your business.

Indochine Counsel represents and advises clients on all legal aspects in the following major areas of expertise:

- Anti-trust & Competition
- Banking & Finance
- Corporate & Commercial
- Energy, Natural Resources & Infrastructure
- Intellectual Property
- Inward Investment
- Labour & Employment
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Real Estate & Construction
- Securities & Capital Markets
- Technology, Media & Telecommunications

A full list of partners, associates and other professionals is available on our website. |

Contact Us

For further information or assistance, please contact the following Indochine professionals:



Thai Gia Han

Associate | Co-head of IP & TMT
Practice Group
E han.thai@indochinecounsel.com



Nguyen Trung Nghia

Legal Assistant
E nghia.nguyentrung@indochinecounsel.com

Ho Chi Minh City

Unit 305, 3rd Floor, Centec Tower
72-74 Nguyen Thi Minh Khai, District 3
Ho Chi Minh City, Vietnam
T +84 28 3823 9640
F +84 28 3823 9641
E info@indochinecounsel.com

Hanoi

Unit 705, 7th Floor, CMC Tower
Duy Tan Street, Cau Giay District
Hanoi, Vietnam
T +84 24 3795 5261
F +84 24 3795 5262
E hanoi@indochinecounsel.com

www.indochinecounsel.com

This Special Alert is designed to provide our clients and contacts with general information of the relevant topic for reference only, without the assumption of a duty of care by Indochine Counsel. The information provided is not intended to be nor should it be relied upon as a substitute for legal or other professional advice.

© 2024 Indochine Counsel | All Rights Reserved.