

Special Alert

ADMINISTRATIVE SANCTIONS FOR CYBERSECURITY AND DATA PROTECTION VIOLATIONS IN VIETNAM: FROM DRAFT DECREE TO FUTURE ENFORCEMENT OUTLOOK

May 2026

Recently, one of the key legislative instruments released for public consultation by the Ministry of Public Security is the *draft Decree on administrative sanctions in the fields of cybersecurity and personal data protection* (the “**Draft**”). This updated Draft, compared with earlier versions that had previously been circulated for consultation but were not formally adopted, marks an important step forward by the Ministry of Public Security in its efforts to further refine the legal framework, keep pace with emerging trends, closely align with practical realities in ensuring compliance with the Law on Cybersecurity, the Law on Personal Data Protection, and relevant implementing regulations.

The Draft has been developed based on a practical and issue-oriented approach, as reflected in its proposed measures to address matters such as the posting of false information in cyberspace, the collection, use, and trading of personal data for illicit gain, etc. In addition, the Draft seeks to remedy the current fragmented, unsystematic framework governing administrative sanctions in the fields of cybersecurity and personal data protection, while also reviewing and adjusting maximum penalties to increase deterrence commensurate with the actual damage and illegal profits generated from violations.

The article will focus on analyzing the main violations in the field of cybersecurity and personal data protection, together with the corresponding administrative sanctions, to help readers gain an overview of the Draft.

Key Takeaways

- **Violations of Personal Data Protection Regulations:** The sanctioning regime in this field applies to data subjects, Personal Data Controllers, Personal Data Processors, Personal Data Controller-cum-Processors, and other involved entities, subject to their respective roles. Key provisions relate to violations of data subjects' rights, consent, illegal trading of personal data, data processing impact assessments, and cross-border data transfer impact assessments.

- **Violations of Regulations on Online Information:** Violations and sanctions related to social network establishment licenses, websites, compliance obligations and responsibilities of service providers and users are also specifically and strictly regulated.
- **Violations of Regulations on Implementation of Cybersecurity Protection Activities:** Requirements for ensuring information cybersecurity, protecting children, and especially data localization, establishing branches or representative offices in Vietnam, impose strict compliance obligations. Therefore, violations may be subject to fines ranging from VND25 million to VND100 million, depending on the nature of the violation.
- **Violations of Regulations on Ensuring Social Security and Anti-Spam:** A key aspect of this section concerns sanctions against the dissemination of false information, as well as violations relating to personal secrets and private life in cyberspace. In addition, with the increasing prevalence of spam content, the proposed sanctions are expected to serve as a significant deterrent against such conduct.

Violations of Regulations on Personal Data Protection

The current Law on Personal Data Protection is considered an important legal document that creates “a steel shield” to protect individuals’ data. However, the effectiveness of enforcement in practice still depends to some extent on further improving comprehensive sanctioning mechanism for violations. In this context, the proposed penalties in the Draft are expected to enhance the feasibility and overall effectiveness of enforcing laws on personal data protection in the future.

Rights of data subjects

Legal regulations require data subjects to protect their own personal data while also respecting and protecting the personal data of others. Accordingly, individuals who violate these obligations may be subject to fines ranging from VND50 million to VND70 million.

In addition, in order to exercise the data subjects’ rights, such as the right to restrict, the right to object, the right to request viewing, editing, etc., the Personal Data Controllers and the Personal Data Controller-cum-Processors must establish appropriate procedures, processes, forms, and ensure that data subjects are informed about such procedures for exercising their rights. In the event of non-compliance with the foregoing requirements, violating entities may be subject to fines ranging from VND 70 million to VND 100 million. In addition, entities involved in data processing activities, depending on actual respective roles, may also be subject to similar fines for failing to implement data subjects’ rights upon lawful requests and in accordance with applicable laws.

Consent and withdrawal of consent

Consent from the data subjects serves as a clear indication of the data subjects’ willingness to allow the processing of their personal data. The validity of such consent depends on the data subjects’ voluntary and full awareness of the data type, processing purpose, the Personal Data Controllers, the Personal Data Controller-cum-Processors, and the data subjects’ rights and obligations. Accordingly, if personal data is processed without the data subjects’ consent, or the data

subjects are compelled to consent for purposes other than those agreed upon, or if data processing continues after the data subjects have withdrawn the consent, the violating individual may be fined from VND50 million to VND70 million. Such fines shall be doubled in the case of organizational violations.

In reality, many entities, particularly enterprises, are processing large volumes of personal data without having established adequate mechanisms to control and demonstrate valid consent. This can easily lead to violations and risks fines ranging from VND70 million to VND100 million for individuals, and double that for organizations. Specifically, this fine applies to the processing of personal data when the data subjects remain silent or unresponsive to requests for consent, or when the Personal Data Controllers or the Personal Data Controller-cum-Processors cannot demonstrate valid consent from the data subjects.

To avoid potential risks of administrative sanctions in the future, entities processing personal data should review all existing data flows, classify data subjects into internal groups (including employees and job applicants) and external groups (including employees of customers and service providers), categorize the personal data being processed (including basic personal data and sensitive personal data) according to each specific processing purpose. On that basis, the development and implementation of procedures for managing consent and withdrawal of consent by data subjects will become more manageable and efficient.

Illegal trading of personal data

Fines ranging from VND50 million to VND70 million will be imposed for the illegal trading of personal data that does not rise to the level of criminal liability. Repeated violations may be subject to fines of up to 5% of the violator's total revenue generated in Vietnam during the preceding fiscal year. However, it should be noted that certain cases of personal data transfer with the data subjects' consent, between departments within the same organization, from the Personal Data Controllers, the Personal Data Controller-cum-Processors transferring to the Personal Data Processors, Third parties for processing, and others in accordance with law, whether fee-based or free of charge, are not considered trading personal data and are therefore not subject to the aforementioned fines.

Data processing impact assessment and cross-border transfer of personal data

The Personal Data Controllers, Personal Data Processors, Personal Data Controller-cum-Processors, may be subject to fines ranging from VND50 million to VND70 million for failing to prepare, retain, or submit personal data processing impact assessment dossier (the "**PDPIA Dossier**") to, or failing to comply with requests for amendment or supplementation from the Ministry of Public Security. In addition, administrative fines ranging from VND70 million to VND100 million may be imposed on entities transferring personal data abroad without preparing, retaining, or submitting the cross-border personal data transfer impact assessment dossier (the "**CPDTIA Dossier**"), failing to notify upon successful transfer, or failing to comply with inspection, amendment, or supplementation requirements issued by the Ministry of Public Security.

Fines may be increased to twofold or fivefold or up to 5% of the total revenue of the preceding financial year in Vietnam if, respectively, personal data of 100,000 to under 1,000,000, or from 1,000,000 to under 5,000,000, or over 5,000,000 Vietnamese citizens or more is disclosed or lost or transferred overseas, depending on the circumstances.

Although the aforementioned regulations on administrative sanctions in the field of personal data protection, particularly those relating to the submission of PDPIA and CPDTIA Dossiers, are currently under public consultation and have not yet officially taken effect, but they may become effective in the near future given the urgency of the regulated field. However, in practice, entities processing personal data continue to encounter significant difficulties in carrying out the procedures for submitting such dossiers, which may create substantial compliance burdens for both data-processing entities and competent authorities responsible for handling registration procedures. Specifically, for direct submissions or via postal services, no official confirming receipt has yet been issued, making it difficult for entities to demonstrate compliance with statutory filing obligations. Meanwhile, neither the National Public Service Portal nor the Ministry of Public Security's Public Service Portal currently provides an online procedure for the submission of the above dossiers. As a result, this issue presents considerable challenges for entities from both legal compliance and operational perspectives.

For now, entities will need to wait for further guidance and specific implementation mechanisms from the Ministry of Public Security. However, given the current context, entities should not remain entirely passive, but should proactively review the personal data flows under their control, prepare the PDPIA and CPDTIA Dossiers to timely adapt to future requirements and updates issued by the Ministry of Public Security.

Violations of Regulations on Online Information

Requirements for licensing, operational compliance and the responsibilities of social network service providers and website operators are mandatory to protect users' rights. Therefore, the Draft aims to tighten operational practices and compliance obligations through more stringent and deterrent sanctions.

Social network establishment license and websites

The term "*Social network establishment license*" as mentioned in the Draft is currently being used under Decree No. 72/2013/ND-CP regulating the management, provision, and use of internet services and online information. However, this decree has expired and been replaced by Decree No. 147/2024/ND-CP. Accordingly, in order to ensure consistency and avoid confusion, the Draft should instead use the terms "*Social network service provision license*" and "*Confirmation of notification of social network service provision*" as prescribed under Decree No. 147/2024/ND-CP to refer to the licenses/notifications applicable to social network services. With this interpretation, the public will need to wait for a more complete and accurate version of the Draft from the competent state authorities. Based on the core spirit and principles that the Draft aims for, it can be understood that penalties may be applied to entities providing social network services without the required licenses or notification as per current regulations.

Accordingly, fines ranging from VND25 million to VND50 million may be applied to acts such as failing to apply for reissuance or using expired licenses, failing to notify when changing ownership or registered office address or sharing links to online information that violates the law, conducting acts of propagating, inciting violence, obscenity, depravity, social evils, etc., on websites. Furthermore, for acts of failing to amend, supplement the license content or providing false, offensive information to other entities, impersonating another entity's website, etc., individuals may be fined from VND50 million to VND75 million. As for providing social network services without the required license, violating individual may result in particularly severe fines ranging from VND125 million to VND175 million.

Responsibilities of service providers and users

It should be noted that organizations and enterprises operating social networks in breach of statutory obligations may face fines ranging from VND50 million to VND175 million, depending on the nature and severity of the violation. Users should likewise remain aware of their responsibilities and exercise caution when using social network services and websites, as violations may result in fines ranging from VND20 million to VND50 million, depending on the nature and severity of the violation.

Violations of Regulations on Implementation of Cybersecurity Protection Activities

Information security assurance in cyberspace

Compliance requirements including user identity verification upon digital account registration, protection of user accounts and information, and server localization in Vietnam for websites and social networks are consistently emphasized in practice. Accordingly, depending on the severity of the violation, non-compliance with these requirements may be subject to fines ranging from VND75 million to VND100 million.

Protection of children in cyberspace

Children are considered one of the most vulnerable groups in the online environment. Current circumstances indicate that children are frequently lured and manipulated by malicious actors in cyberspace into engaging in unlawful activities. Therefore, establishing and enforcing sanctions against violations of regulations on child protection in cyberspace is considered both necessary and important.

Accordingly, service providers that fail to implement content control measures, prevent the sharing and removal of content harmful to children may be subject to fines ranging from VND25 million to VND50 million. Any individual engaging in the posting, dissemination, sharing, exchange, use of information, images, audio containing pornographic, obscene, violent, or otherwise harmful content affecting the honor, reputation, dignity, health, or normal development of children may face fines ranging from VND50 million to VND75 million. In addition, individuals who fail to cooperate with competent authorities, or who engage in acts of incitement, inducement, coercion, manipulation of children into following, sharing, or disseminating harmful content, or participating in other unlawful activities, may be subject to fines ranging from VND70 million to VND100 million.

Data localization, establishment of branches or representative offices in Vietnam

Currently, in addition to data localization requirements for users in Vietnam, foreign enterprises may also be required to establish a branch or representative office in Vietnam if operating in the fields of telecommunications services, data storage, sharing in cyberspace, e-commerce, social networks, among others. Accordingly, the regulation of Draft clearly reflects the approach that non-compliance with these requirements may result in fines ranging from VND75 million to VND100 million.

Violations of Regulations on Ensuring Social Security and Anti-Spam

Under the Draft, violations of regulations on ensuring public order and safety in cyberspace that do not rise to the level of criminal liability may be subject to administrative sanctions. The penalties mainly apply to acts such as disseminating fabricated or false information, infringing upon the honor, reputation, dignity of others, impersonating others or disseminating information that adversely affects the lawful rights and interests of others, or creating, disclosing personal secrets and private life information that adversely affects others in cyberspace. Common fines range from VND10 million to VND30 million for individuals and may be doubled for violating organizations. In the context of the increasing prevalence of false information and privacy violations in cyberspace, the proposed regulations under the Draft are viewed as positive indication of a stricter sanctioning mechanism that could be implemented in the future.

In addition, another important issue in the Draft is sanctions for violations of anti-spam regulations, particularly in light of the increasing volume of spam content which not only waste users' time but also adversely affect their rights and interests. Accordingly, the Draft relatively clearly categorizes specific violations and the corresponding sanctions applicable to individuals. Notably, the proposed fines ranging from VND5 million to VND30 million may be imposed for sending advertising emails, messages, making calls without the recipients' consent or after the recipient has refused consent, or for failing to provide a mechanism for receiving and processing spam notifications, failing to verify consent, or failing to provide guidance on how to combat spam. The fines may increase, specifically from VND60 million to a maximum of VND200 million, if an individual engages in acts such as sending spam emails or messages, distributing malicious software, generating multiple missed calls for profit-making or advertising purposes without implementing a system for receiving and processing opt-out requests, or fails to block, revoke phone numbers used for distributing spam messages or calls. Compared with current regulations in the information technology sector, the proposed penalties also demonstrate a similarly deterrent effect.

Conclusion

Controlling, deterring, limiting, and progressively eliminating violations are clear objectives that the Ministry of Public Security seeks to achieve through the Draft. Compared to previously fragmented regulations, the Draft has taken an initial step toward establishing a relatively clear and structured sanctioning framework, thereby helping to address inconsistencies in enforcement and enhance the transparency of the legal system. This serves as an important foundation for reshaping compliance behavior among relevant stakeholders, particularly in the context where violations are becoming increasingly sophisticated, organized, and prevalent in the digital environment.

This development also demonstrates the strong commitment of the competent authorities to improving the effectiveness of law enforcement, with a view to building a practical and enforceable legal framework that closely aligns with regulatory needs and real-world application. From a public perspective, the continued refinement of the Draft not only reinforces confidence but also raises expectations for a sufficiently robust and flexible enforcement mechanism, ensuring that sanctions in the fields of cybersecurity and personal data protection can be effectively implemented in the near future.

About Indochine Counsel

Established in October 2006, Indochine Counsel is a premier commercial law firm in Vietnam. We're ideally positioned to help international investors and foreign firms navigate the legal landscape in one of Asia's most dynamic and exciting countries. We also take pride in our services for domestic clients searching for opportunities abroad. With over 45 lawyers and staff in two offices, Ho Chi Minh City and Hanoi, Indochine Counsel offers expertise in a dozen practice areas assisting you throughout the entire life cycle of your business. We're your trusted partner in Vietnam for international and domestic legal solutions.

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

Contact Us

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



Thai Gia Han

Senior Associate | Head of IP & TMT
Practice Group

E han.thai@indochinecounsel.com



Nguyen Trung Nghia

Junior Associate

E nghia.nguyentrung@indochinecounsel.com

Ho Chi Minh City

Unit 305, 3rd Floor, Centec Tower
72-74 Nguyen Thi Minh Khai, Xuan Hoa Ward
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 Ward
Hanoi, Vietnam

T +84 24 3795 5261
F +84 24 3795 5262
E hanoi@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.

© 2006 – 2026 Indochine Counsel. All Rights Reserved



You can reach us at
[Indochinecounsel.com](https://www.indochinecounsel.com)



LinkedIn



Facebook



YouTube