

# Legal Update

August 2023

## Cybersecurity and Administration Sanctions: The Third Draft Decree Explained

In the last few months, the Government issued two significant regulations on cybersecurity and personal data protection which are (i) Decree 53/2022/ND-CP providing guidance on the implementation of the Law on Cybersecurity (“**Decree 53**”) and (ii) Decree 13/2023/ND-CP on personal data protection (“**Decree 13**”).

To ensure the enforcement of the abovementioned regulations on cybersecurity and personal data protection, on 31 May 2023, the Ministry of Public Security (“**MPS**”) circulated a 3rd version of the draft decree on cybersecurity administrative sanctions (“**Draft CASD**”) for public consultation. The Draft CASD features an updated list of non-compliances with the cybersecurity and data privacy regulations and also replaces certain regulations covered under the existing Decree 15/2020/ND-CP and Decree 14/2022/ND-CP on administrative sanctions against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions.

Some of the key highlights from the Draft CASD are as follows:

### 1. Application

The Draft CASD will not only apply to entities providing services in Vietnam related to telecommunications, internet, and content services in cyberspace, information technology, cybersecurity, cyberinformation security, but also to all domestic and foreign individuals and organizations that are involved in processing personal data in Vietnam and/or of Vietnamese citizens. The entities covered by this broad scope of application of Draft CASD should take steps to ensure they comply with Decree 53 and Decree 13, and to avoid any censure once the regulation is officially issued.

In brief, Draft CASD governs administrative sanctions in relation to the 5 main areas: (i) information security; (ii) personal data protection; (iii) cyberattack prevention; (iv) implementation of cybersecurity protection activities; (v) prevention and protection acts against using cyberspace, information technology and electronic means to violate the law on social order and safety.

### 2. Overview of Penalties

The Draft CASD introduces 3 classes of penalties with monetary fines being the principal form of penalties. The fines can be applied in addition to, or in lieu of further sanctions or corrective actions.

The additional sanctions will depend on the nature and severity of the violation and can take the form of suspension of operations or business licenses, confiscation of violating exhibits and expulsion from Vietnam.

The remedial actions include removal or modification of offending programs or software or products or equipment or its associated information or features, deletion or destruction of offending data, removal or rectification of distorted data, revocation of subscriber information or public apology.

Intentionally committing an infringement, failing to comply with the supervisory authority's request for remedial action, or failing to cooperate with the authorities can increase penalties.

For aggravated violations such as processing personal data for marketing and advertising activities without the data subject's consent, sale and purchase of personal data and failure to file the impact assessment report with the authorities could attract fines of up to 5% of an organization's revenue for the preceding financial year or profits in Vietnam in addition to any other remedial measures or sanctions.

The Draft CASD will give the Vietnamese supervisory authorities the power to impose sanctions on persons and entities who violate either or both the cybersecurity and data protection regulations based on its assessment of the severity of the violation. Relevant authorities who have the power to impose administrative sanctions for violations will depend on the nature and severity of the violation include competent officials of the People's Public Security, People's Committees at all levels, Inspectors of the Ministries, Border Guards, and Vietnam Coast Guard, which the Director of the Department of Cybersecurity and High-Tech Crime Prevention (A05) being the regulator with the highest authority.

### 3. Specific categories of violations

#### ***Violation of obligations relating to information security***

Based on the assessment of the authorities, violations of information security assurance include dissemination, storage, and production of fake, misleading, illegal or untrue content, and the penalties that may be imposed include:

- (i) A fine of up to VND 20 million (approx. USD842) for individuals and VND 40 million (approx. USD1,684) for organizations spreading and storing information with anti-State content.
- (ii) A fine of up to VND 40 million (approx. USD1,684) for individuals and VND 80 million (approx. USD3,367) for organizations (a) creating and spreading information with anti-State content; (b) disseminating information that offends the honor and dignity, affects the legitimate rights and interests of other individuals and organizations, false information in business activities, and causes confusion in public opinion about ethnicity, social ethics and public health; (c) failure to implement management and technical measures to coordinate with the competent authorities to prevent and remove the infringing content.
- (iii) A fine of up to VND 60 million (approx. USD2,525) for individuals and VND 120 million (approx. USD5,051) for organizations (a) creating information that offends the honor and dignity affecting the legitimate rights and interests of other individuals and organizations, false information in business activities, false information causing confusion in public opinion about ethnicity, social ethics and public health; (b) failure to comply with the requirements of the competent authorities to arrange necessary technical conditions, prevent, stop providing services or mobilize resources when there is a violation.
- (iv) A fine of up to VND 80 million (approx. USD3,367) for individuals and VND 160 million (approx. USD6,734) for organizations that set up social networking sites, accounts, specialized pages and groups to create and post false and misleading information affecting the legitimate rights and interests of organizations and individuals.
- (v) Suspension of business for 1-3 months could also be imposed on the violations related to the establishment of digital information pages, social networks or accounts, online groups for creating, publishing the abovementioned information.

#### ***Violation of obligations related to personal data protection***

The Draft CASD provides a comprehensive list of offences that covers almost all obligations that organizations and individuals are required to comply with under Decree 13 when processing personal data in Vietnam and/or of Vietnamese citizens, such as violations of personal data protection, failure to address personal data owner rights, or having an appropriate data protection governance framework including assigned personnel or department when processing sensitive personal data. The fines are based on the specific list in the Draft CASD with some infringements carrying a lower-level penalty whereas infringements on certain violations range from VND 20 million (approx. USD842) to VND 160 million (approx. USD6,734). For more severe violations, the authorities have the power to impose additional sanctions and remedies including the withdrawal of business license, suspension of data processing or irrevocably destroying/deleting personal data for related breaches, including but not limited to: principles of personal data protection, right of data subject, consent or retention/ deletion/ destruction of personal data.

Specifically, a fine of up to VND 200 million (approx. USD8,418), increased to five times of this amount or up to 5% of revenue with additional sanctions and remedies will be applied to violations regarding:

- (i) the use of personal data for marketing, recommending and advertising products and services;
- (ii) the illegal collection, transfer and purchase of personal data;
- (iii) obligation to conduct a personal data process impact assessment;
- (iv) obligations to conduct a cross-border transfer of personal data.

## ***Violation of obligations related to cyber-attack protection and response***

This rule imposes fines on violations related to (i) deliberately spreading, manufacturing, purchasing harmful computer programs on the Internet and telecommunication network; (ii) using cyberspace (sharing, commenting) for terrorist activities or threats of terrorism; or (iii) coordinating with the competent authorities on taking action against the relevant violations with fines ranging from VND 40 million (approx.USD1,683) to VND 160 million (approx. USD6,734) and the withdrawal of business license for 12-18 months. Delaying or obstructing measures taken by competent authorities or supporting terrorism online will also result in a fine of up to VND 200 million (USD8,418).

## ***Violation of obligations related to cybersecurity protection***

Violations related to cybersecurity protection mainly involve intentionally performing illegal acts or failing to comply with requests from authorities, which include:

- (i) Intentionally/assisting in spreading, obstructing, infiltrating or affecting the cybersecurity;
- (ii) Failing to authenticate information when users register for digital accounts;
- (iii) Delaying, obstructing, or failing to take measures at the request of relevant authorities;
- (iv) Failing to perform, coordinating to perform when requested by the cybersecurity task force.

A notable point is that the violations specified herein will be a crucial basis for the supervisory authorities to impose data localization or setting up branches or representative offices in Vietnam according to Decree 53, which obligation shall be fined up to VND 200 million (approx. USD8,418) with additional sanctions and remedial measures to be imposed if the organization fails to comply.

## ***Violation of obligations related to the use of cyber space, information technology, electronic media***

Other violations in the Draft CASD mainly relate to activities in cyberspace, information technology and electronic media inciting anti-state, distorting in order to offend and slander other organizations and individuals, infringing upon privacy rights, the economic management order and affecting the social order. Violations related to authentication, identification and digital account protection will also be fined up to VND120 million (approx. USD5,051) for organizations.

## **4. Concluding remarks**

As the regulations on personal data protection came into force on 1 July 2023, we expect that this decree on cybersecurity administrative sanctions will be issued in the coming months. It will result in an increase in enforcement actions in the personal data space. Notably, a violation that is liable for punishment can be detected through inspection activities conducted by the relevant authorities or by customers or potential customers who escalate their dissatisfaction to the authorities or through a review of the mandatory filing of an organization's processing activities or cross-border transfer activities. As such, all businesses should in the coming weeks become familiar with their statutory obligations to comply and to avoid penalties.

If you have any questions or require any additional information, please contact [Ms. Amarjit Kaur](#) or [Ms. Nguyen Thi Hoang Trang](#) of KPMG Law in Vietnam.

## **Contact us**

### **Hanoi**

46<sup>th</sup> Floor, Keangnam Landmark 72,  
E6 Pham Hung, Me Tri, Nam Tu Liem  
T +84 (24) 3946 1600

### **Ho Chi Minh City**

10<sup>th</sup> Floor, Sun Wah Tower,  
115 Nguyen Hue, Ben Nghe, District 1  
T +84 (28) 3821 9266

### **Da Nang**

Unit D3, 5<sup>th</sup> Floor, Indochina Riverside Towers,  
74 Bach Dang, Hai Chau I, Hai Chau  
T +84 (236) 351 9051

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG Limited, KPMG Tax and Advisory Limited, KPMG Law Limited, KPMG Services Company Limited, all Vietnamese one member limited liability companies and member firms of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.



Scan to visit our website: [kpmg.com.vn](https://kpmg.com.vn)

Email: [kpmghcmc@kpmg.com.vn](mailto:kpmghcmc@kpmg.com.vn)