



GLOBAL VIETNAM
LAWYERS

LEGAL ALERT

No. 05 | August 2026

**Decree No. 330/2026/ND-CP:
Key Personal Data
Protection Issues for
Businesses**



On 19 August 2026, the Government issued Decree No. 330/2026/ND-CP ("**Decree 330**") on administrative sanctions for violations in the fields of cybersecurity and personal data protection ("PDP"). The Decree takes effect immediately from the date of issuance.

Decree 330 introduces various penalties for violations relating to the collection, use, storage and processing of personal data. Importantly, many of these violations may arise from businesses' day-to-day operations.

Below are the key issues and 13 categories of violations that businesses should pay attention to:

1. Applicable scope – Cyberspace has no physical borders

Decree 330 has a **broad scope of application**. It applies not only to violations occurring within the territory and territorial waters of Vietnam, but also to violations committed in **cyberspace under Vietnam's jurisdiction**.

Importantly, its scope may cover **foreign businesses** providing telecommunications, Internet, digital content, cross-border or cybersecurity services where they are directly involved in activities relating to the processing of Vietnamese citizens' personal data.

Households, household businesses and residential communities that commit violations also fall within the scope of the Decree and are subject to penalties applicable to individuals.

Accordingly, the fact that a business has no physical presence or headquarters in Vietnam does not necessarily place it outside the scope of Decree 330/2026 if it carries out personal data processing activities falling within the Decree's scope.

2. Penalties can be substantial

The maximum fine for ordinary violations is VND 3 billion.

For certain serious violations such as (i) Illegal purchase or sale of personal data: a fine of up to 10 times the illegal proceeds; and (ii) Violations relating to cross-border

transfers of personal data: a fine of up to 5% of the business's total revenue in Vietnam in the immediately preceding financial year.

The above fines apply to organizations. Individuals are subject to fines equal to 50% of the fines applicable to organizations.

3. Silence cannot automatically be treated as consent

Businesses must not automatically treat a user's silence or failure to respond as consent to the processing of personal data.

A violation may result in a fine of up to VND 70 million.

4. Collecting data beyond the permitted purpose or scope

Businesses must collect personal data within the specific and clearly defined scope and purpose, and on a lawful basis.

Violations may result in fines of (i) VND 30–50 million for ordinary personal data; or (ii) VND 50–80 million for sensitive personal data.

The unlawful use of technologies or technical methods to collect personal data may result in fines of VND 100–800 million, depending on the volume of data collected.

5. Improper processing of biometric data

Businesses processing biometric data must implement appropriate security measures for devices used to store and transmit such data.

A violation may result in a fine of VND 50–70 million.

Using biometric data beyond its original purpose without obtaining consent may result in a fine of up to VND 150 million.

6. Installing cameras without proper notice

When using cameras or audio/video recording devices in public spaces or areas where customer services are provided, businesses must provide clear physical or electronic notices/warnings.

A violation may result in a fine of VND 10–20 million.

7. Excessive collection or use of data in recruitment and employment

Businesses should ensure that the collection and use of candidates' and employees' personal data are appropriate for legitimate recruitment and employment management purposes.

In particular, failure to delete or destroy data of unsuccessful candidates as required: VND 20–50 million; and using monitoring software, cameras or other data-collection devices in the workplace without notifying employees: VND 50–70 million.

8. Improper advertising and behavioral tracking

Businesses should provide customers with mechanisms to opt out of receiving advertisements and withdraw consent to the sharing of personal data for advertising purposes.

A violation may result in a fine of VND 30–50 million.

In particular, tracking customers through websites, applications or other activities for behavioral advertising, targeted advertising or personalized advertising without consent may result in a fine of VND 50–70 million.

9. Failure to promptly report data incidents

Where an incident results in the disclosure or loss of sensitive personal data, businesses must comply with applicable notification obligations, including the 72-hour notification deadline from the time the incident is detected, where such notification is required.

Late notification or inaccurate reporting of the scale of the incident may result in a fine of VND 50–70 million.

10. Failure to appoint personnel or a department responsible for personal data protection

Businesses are required to designate a qualified department or personnel responsible for personal data protection, with such appointment being properly documented as required by law.

A violation may result in a fine of VND 20–30 million.

11. Failure to prepare a Personal Data Processing Impact Assessment (DPIA)

Where a business is required to prepare a Personal Data Processing Impact Assessment dossier but fails to prepare, maintain or submit it within the prescribed time limit, it may be subject to a fine of VND 20–30 million.

For cross-border transfers of personal data, failure to prepare or timely submit

the relevant impact assessment dossier may result in a fine of VND 30–50 million.

12. Failure to establish procedures for handling data subject requests

Businesses should establish appropriate procedures, processes and forms for handling requests from data subjects, including requests to withdraw consent, correct personal data, access or receive personal data, or delete personal data.

Valid requests must be handled within two working days in accordance with the applicable regulations.

A violation may result in a fine of VND 10–20 million.

13. Use of AI/Big Data without adequate safeguards

Where Big Data or AI is used to make automated decisions, businesses should ensure that, where required by law, (i) appropriate human oversight mechanisms are established, (ii) users are allowed to request human review of automated decisions; and (iii) users are informed and provided with an explanation of the operation of the algorithm and the impact of the automated decision on them.

Violations may result in fines of (i) VND 50–100 million for certain failures relating to supervision and human review mechanisms; and (ii) VND 50–70 million for failure to provide the required notification or explanation.

14. Failure to conduct periodic compliance assessments

Certain businesses, including those processing large volumes of data or using AI, blockchain or cloud computing, as well as businesses operating in the finance and banking sector, may be required to conduct annual personal data protection compliance assessments.

A violation may result in a fine of VND 20–50 million, depending on the applicable circumstances.

What should businesses do now?

Decree 330 demonstrates that personal data protection compliance is not solely an issue for a company's legal or IT department. It directly affects many day-to-day activities, including recruitment, marketing, advertising, employee monitoring, camera surveillance, data storage, incident response and the use of AI.

Businesses should proactively:

1. Review all personal data collection and processing activities;
2. Review their mechanisms for obtaining, recording and managing consent;
3. Review the processing of sensitive personal data and biometric data;
4. Assess compliance requirements relating to DPIAs and cross-border data transfers;
5. Establish clear procedures for handling data subject requests and data breaches;
6. Review the use of cameras, employee monitoring tools, cookies, AI and advertising technologies; and
7. Identify any applicable requirements for periodic personal data protection compliance assessments.

Disclaimer: This Legal Alert is provided for general information purposes only and does not constitute legal advice in relation to any specific case or circumstances. Businesses should conduct a review of their actual operations and the applicable regulations to determine their specific compliance obligations.

2026



CONTACT US

info@gvlawyers.com.vn

Ho Chi Minh City Office

8th, Centec Tower,
72 – 74 Nguyen Thi Minh Khai Street,
Xuan Hoa Ward, Ho Chi Minh City, Vietnam
Tel: +84 (28) 3622 3555

Hanoi Office

10th, CDC Building
25 Le Dai Hanh Street,
Hai Ba Trung Ward, Hanoi, Vietnam
Tel: +84 (24) 3208 3555

The contents of the Legal Alert neither constitute legal advice nor necessarily reflect the opinions of our firm or any of our attorneys or consultants. The Legal Alert provides general information, which may or may not be complete or up to date at the time of reading. The content is not intended to be used as a substitute for specific legal advice or opinions. Please seek appropriate legal advice or other professional counselling for any specific issues you may have. We, GV Lawyers, expressly disclaim all liabilities relating to actions whether taken or untaken based on any or all contents of the newsletter.



+84 28 3622 3555



www.gvlawyers.com.vn