



Shape the future  
with confidence

**Legal Alert**

October 2026

Visit other Alerts [here](#).

# Decree 330/2026/ND-CP providing sanctions for Personal Data Protection Law violations

This Legal Alert highlights the key enforcement risks and compliance implications arising from Decree 330/2026/ND-CP, Vietnam's first dedicated administrative sanctions regime for personal data protection, including the scope of application, sanction framework, and practical areas of regulatory focus for businesses.

On 19 August 2026, the Government issued Decree No. 330/2026/ND-CP on administrative sanctions in the fields of cybersecurity and personal data protection (Decree 330), which took effect immediately upon issuance. In light of this event, Vietnam now has a dedicated and comprehensive personal data protection framework covering substantive obligations, implementation requirements and enforcement mechanisms.

For businesses, Decree 330 marks a significant shift from a compliance framework focused primarily on obligations to one backed by a dedicated sanctions regime. The new framework introduces monetary penalties, additional sanctions and remedial measures for a broad range of personal data protection violations, with potential implications for both Vietnamese entities and foreign organisations involved in processing personal data connected to Vietnam.

This Legal Alert highlights:

- The scope of entities and activities subject to Decree 330
- The principal violations most likely to attract regulatory scrutiny
- The applicable sanction framework, including fixed fines, proceeds-based penalties and revenue-based penalties
- Key enforcement and compliance risks arising from the new regime
- Practical steps businesses should consider to prepare for inspections and enforcement actions

## 1. Overview

For three years, Decree No. 13/2023/ND-CP dated 17 April 2023 and, more recently Law No. 91/2025/QH15 on personal data protection (PDPL) focused on obligations and has not developed a complete sanction regime. Enterprises know what their compliance obligations are under the laws, but is unclear on what the sanctions will be when they do not comply.

That meant regulators reached for whatever tool was closest at hand. There were multiple major enterprises fined for denying customers a genuine choice over whether their personal data could be used for marketing, or giving users incomplete and potentially misleading information about how their data was collected and used. These were, in substance, personal data violations. They were prosecuted through a consumer-protection lens, because the data protection law itself had no dedicated sanctions regime to reach for yet.

On 19 August 2026, Decree 330 took effect. There is no transition period.

With Decree 330, Vietnam's personal data protection framework is, for the first time, a complete architecture rather than a work in progress: PDPL sets out the rights and obligations, Decree No. 356/2025/ND-CP dated 31 December 2025 (Decree 356) guides on how to comply, and Decree 330 spells out the sanctions when a business does not comply.

Although Decree 330 regulates both cybersecurity and personal data protection, this Legal Alert focuses solely on the sanctioning provisions relating to personal data protection, ranging from Article 39 to Article 71.

## 2. Broad scope of application

Decree 330 applies broadly: to Vietnamese and foreign individuals and organizations. More particularly, it reaches foreign entities that directly process, or are otherwise involved in processing, the personal data of Vietnamese citizens and of Vietnamese-origin individuals residing in Vietnam who hold an identity certificate but have not yet had their nationality determined.<sup>1</sup>

## 3. The statute of limitation

The statute of limitations for administrative sanctions in this field is one year.<sup>2</sup> For a completed violation, that year starts running from the date the obligation was actually fulfilled, or the date a competent authority confirms the violation has ended.<sup>3</sup>

## 4. Categories of violations

Decree 330 establishes a comprehensive administrative sanctioning framework for personal data protection violations, covering non-compliance relating to compliance documentation and procedures, governance and internal policies, resources and personnel responsible for personal data protection, as well as technical and data security measures. This demonstrates that compliance risks are not limited to documentation and reporting requirements, but extend across an organization's governance framework, personnel, and data protection measures.

In practice, many violations may arise in day-to-day operations and are relatively common in business activities, including:

- Failure to ensure that data subjects provide separate consent for each processing purpose
- Failure to retain evidence or logs demonstrating the obtaining of consent

---

<sup>1</sup> Article 2 Decree 330

<sup>2</sup> Article 3.1 Decree 330

<sup>3</sup> Article 3.2 Decree 330

- Failure to establish procedures and templates for receiving and handling data subject rights requests
- Failure to implement mechanisms to control access to, use of, or sharing of data among internal departments
- Failure to prepare, update, or periodically submit personal data processing impact assessment dossiers
- Failure to delete or destroy personal data of unsuccessful job applicants
- Failure to provide a mechanism for data subjects to opt out of receiving advertising content
- Assigning personnel responsible for personal data protection who do not meet the required qualifications, experience, or appropriate training in personal data protection

## 5. Areas for consideration

Although Decree 330 is primarily an administrative sanctions regulation, it also contains a number of provisions that further interpret, tighten, or expand upon the requirements under the PDPL and Decree 356.

| Aspect                                                                      | PDPL and Decree 356                                                                                                                                                                                                                                                                                                                           | Decree 330                                                                                                                                                              | Implications                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processing personal data of children aged 7 and above                       | The PDPL regulates that the processing of the personal data of children aimed to disclose information on the private life or personal secrets of children aged 7 or older must receive the consent of the children and their legal representatives. <sup>4</sup>                                                                              | Sanctions imposed on processing the personal data of children aged 7 and above without the consent of both the child and the child's legal representative. <sup>5</sup> | Unlike the PDPL, the relevant sanctioning provision under Decree 330 is not expressly limited to processing for the purpose of publishing or disclosing a child's private life or personal secrets, potentially suggesting a broader application of the dual-consent requirement. |
| Age verification requirement for the processing of children's personal data | The PDPL does not expressly require organisations to verify a child's age before processing the child's personal data. However, Article 24.2 of the PDPL requires the consent of both the child and the child's legal representative where personal data is processed for the purpose of publishing or disclosing information relating to the | Sanctions imposed on failing to implement an age-verification process before processing children's personal data. <sup>6</sup>                                          | Decree 330 introduces an additional obligation to verify a child's age prior to processing the child's personal data.                                                                                                                                                             |

<sup>4</sup> Article 24.2 PDPL

<sup>5</sup> Article 60.1(c) Decree 330

<sup>6</sup> Article 60.1(a) Decree 330

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        | child's private life or personal secrets.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Retention period                       | <p>The PDPL requires ensuring that personal data is stored for a period in conformity with the personal data processing purpose.<sup>7</sup></p> <p>Decree 356 requires organizations and individuals transferring personal data under Points (a), (c), and (d), Clause 1, Article 17 of the PDPL must enter into a personal data transfer agreement with the personal data recipient, which must specify, the personal data processing period.<sup>8</sup></p>                               | Sanctions imposed on transferring personal data under Points (a) and (d), Clause 1, Article 17 of the PDPL for a fee for the purpose of providing services to, or serving the legitimate interests of, the data subject, without specifying a personal data retention period appropriate to the transfer purpose. <sup>9</sup> | For this case, businesses should comprehensively specify a retention period appropriate for the purpose of the transfer in the personal data transfer agreement.                                                                                                                                                                                                                                                               |
| Affiliate advertisement                | <p>The PDPL requires organizations and individuals using personal data for behavioral, targeted, or personalized advertising must have methods for permitting personal data subject matters to refuse to share data.<sup>10</sup></p> <p>Decree 356 further guides this by prohibiting the establishment of default consent mechanisms or creation of unclear or misleading instructions that cause confusion between consent and non-consent for the personal data subject.<sup>11</sup></p> | Sanctions imposed on establishing a default opt-in mechanism for the disclosure of a data subject's personal data to an affiliate advertising network. <sup>12</sup>                                                                                                                                                           | While neither the PDPL nor Decree 356 specifically refers to affiliate advertising networks, Decree 330 expressly introduces sanctions for the use of default consent mechanisms in this context. Obtaining consent in connection with the provision of personal data to affiliate advertising networks and clearly establish a method that allows personal data subjects to refuse the sharing of their data are recommended. |
| Data obtained from public surveillance | The PDPL permits the collection and processing of personal data obtained through audio and video                                                                                                                                                                                                                                                                                                                                                                                              | Sanctions imposed using personal data, images or voice recordings obtained                                                                                                                                                                                                                                                     | Decree 330 addresses a scenario not expressly covered by the PDPL by imposing sanctions on                                                                                                                                                                                                                                                                                                                                     |

<sup>7</sup> Article 3.3 PDPL

<sup>8</sup> Article 7.1(c) Decree 356

<sup>9</sup> Article 52.2(c) Decree 330

<sup>10</sup> Article 28.8(b) PDPL

<sup>11</sup> Article 6.3 Decree 356

<sup>12</sup> Article 63.1(c) Decree 330

|                |                                                                                                                             |                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| camera systems | recording in public places or public activities without the data subject's consent in specific circumstances. <sup>13</sup> | through public surveillance camera systems for commercial purposes, behavioural analytics, or automated facial recognition for profiling without the data subject's valid consent. <sup>14</sup> | the use of personal data obtained through public surveillance camera systems for commercial purposes, behavioural analytics, or automated facial recognition for profiling without valid consent.<br><br>Businesses should review the purposes for which data obtained from public surveillance camera systems is used and obtain lawful consent before using such data for the purposes specified above. |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 6. The sanctions

### 6.1. Principal sanctions:

- Fixed brackets: Most violations carry a straightforward VND range. Processing personal data without valid consent, for example, is punishable by up to VND50 million;<sup>15</sup> continuing to process data after a valid withdrawal or restriction request, or treating silence as consent runs VND50-VND70 million.<sup>16</sup>
- Proceeds-based multiplier (2x-10x): This is applied to the illegal trading of personal data (unauthorised sale, paid sharing not in line with the data transfer agreement or data subject's consent).<sup>17</sup>
- Revenue-based percentage (1%-5%): This is applied to a narrow category of serious violations, principally cross-border transfers that result in the loss or leakage of the personal data of ten thousand or more Vietnamese citizens.<sup>18</sup> The maximum is 5% of the prior year's revenue; where there is no prior-year revenue, the ceiling defaults to VND3 billion.<sup>19</sup>

| Violation                                                                            | Maximum penalty (organizations) |
|--------------------------------------------------------------------------------------|---------------------------------|
| Deletion/destruction failures involving children's data processed beyond its purpose | Up to VND200 million            |

<sup>13</sup> Article 32.1 PDPL

<sup>14</sup> Article 71.2(a) Decree 330

<sup>15</sup> Article 43.1 Decree 330

<sup>16</sup> Article 43.2 Decree 330

<sup>17</sup> Article 53.1 Decree 330

<sup>18</sup> Article 56.3 Decree 330

<sup>19</sup> Article 7.4 Decree 330

|                                                                                           |                                                         |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Failure to implement measures preventing personal data protection violations              | Up to VND80 million                                     |
| Failure to meet statutory deadlines for a data subject's request                          | Up to VND40 million                                     |
| Illegal trading of personal data                                                          | Up to VND3 billion                                      |
| Cross-border transfer resulting in loss/leakage of data of 1,000,000+ Vietnamese citizens | Up to 5% of prior-year Vietnam revenue, or VND3 billion |

- 6.2. Additional sanctions: Beyond fines, Decree 330 allows suspension of the operation of information systems, application platforms, or personal data processing activities for a specified period; revocation of relevant licences or certificates; confiscation of instruments and means used for the violation.<sup>20</sup>

Remedial measures: compulsory fulfillment of data subject rights; compulsory correction or deletion of unlawfully processed personal data; compulsory disgorgement of unlawful gains; compulsory notification to, or public apology to, affected individuals; compulsory correction of false or misleading information.<sup>21</sup>

Notably, the proceeds-based multiplier should not be confused with the disgorgement remedy, as the two mechanisms apply in different circumstances and are calculated on different bases. The 2x-10x multiplier monetary fine is specifically applicable to the illegal purchase or sale of personal data and is calculated based on the gross transaction value evidenced by contracts, invoices, payment records, message logs, electronic transaction records, bank statements, e-wallet records, or other materials directly relating to the transaction, without deduction of any costs incurred. By contrast, disgorgement of unlawful gains is a remedial measure that may apply to unlawful collection, processing, use, or transfer of personal data outside the context of illegal data trading. In such cases, the amount subject to disgorgement is determined based on the total revenue actually generated from business activities that utilised unlawfully collected, processed, used, or transferred personal data, also without deduction of any costs or expenses incurred during the violation.<sup>22</sup>

## 7. What businesses should do

Since 19 August 2026, the risk of administrative sanctions has become a reality for any non-compliance with the Personal Data Protection Law and Decree 356. With the authorities now equipped with a complete legal basis to conduct inspections, investigations, and impose administrative sanctions, delays in implementing compliance measures may expose businesses to significant legal, financial, operational, business, and reputational risks.

Better late than never, now is the time for businesses to act. Priority actions should include assessing the current compliance status; identifying gaps in data governance, impact assessment dossiers, data subject consent management, data subject rights procedures, and cross-border data transfer requirements; and strengthening governance structures, personnel responsible for personal data protection, as well as technical and data security measures. Taking

<sup>20</sup> Article 4.2 Decree 330

<sup>21</sup> Article 5 Decree 330

<sup>22</sup> Articles 6.2 and 53.1 Decree 330

proactive remedial actions now can significantly reduce enforcement risks and enhance a business's ability to demonstrate compliance efforts during inspections or audits by competent authorities.

With the sanctioning framework now officially in force, EY Law Vietnam Limited Liability Company stands ready to assist businesses in assessing compliance risks, addressing compliance gaps, and developing a practical and effective roadmap to meet the requirements of the Personal Data Protection Law, Decree 356 and Decree 330 in a manner aligned with their business operations.



Shape the future  
with confidence

Contacts

## Ho Chi Minh City Office



**Robert King | EY Vietnam, Laos, Cambodia Tax Leader**  
EY Consulting Vietnam Joint Stock Company  
[robert.m.king@vn.ey.com](mailto:robert.m.king@vn.ey.com)



**Hieu Duy Nguyen | Law Leader and Managing Director**  
EY Law Vietnam Limited Liability Company  
[hieu.d.nguyen@vn.ey.com](mailto:hieu.d.nguyen@vn.ey.com)



**Robert Tran | Partner**  
EY Digital & Cyber Company Limited  
[robert.tran@vn.ey.com](mailto:robert.tran@vn.ey.com)



**Thach Thi Cam Tran | Director**  
EY Law Vietnam Limited Liability Company  
[thach.cam.tran@vn.ey.com](mailto:thach.cam.tran@vn.ey.com)

## Hanoi Office



**Anh Thuy Pham | Associate Partner**  
EY Law Vietnam Limited Liability Company  
[anh.thuy.pham1@vn.ey.com](mailto:anh.thuy.pham1@vn.ey.com)



**Linh Hoang Anh Nguyen | Director**  
EY Law Vietnam Limited Liability Company  
[linh.hoang.anh.nguyen@vn.ey.com](mailto:linh.hoang.anh.nguyen@vn.ey.com)

## Japanese Business Services (JBS)



**Takahisa Onose | EY Vietnam, Laos, Cambodia JBS Leader**  
Ernst & Young Vietnam Limited  
takahisa.onose@vn.ey.com



**Takaaki Nishikawa | Associate Partner**  
EY Consulting Vietnam Joint Stock Company  
takaaki.nishikawa@parthenon.ey.com

## Korean Business Services (KBS)



**Binh Thanh Phan | EY Vietnam, Laos, Cambodia KBS Leader**  
EY Consulting Vietnam Joint Stock Company  
binh.thanh.phan@parthenon.ey.com



**Kyung Hoon Han | Associate Partner**  
Ernst & Young Vietnam Limited  
kyung.hoon.han@vn.ey.com

## Chinese Business Services (CBS)



**Truong Duc Le | Vietnam, Laos, Cambodia CBS Leader**  
Ernst & Young Vietnam Limited  
truong.duc.le@vn.ey.com



**Owen Tsao | Director**  
Ernst & Young Vietnam Limited  
owen.tsao@vn.ey.com



**Trinh Kiet Luong | Assistant Director**  
Ernst & Young Vietnam Limited  
trinh.kiet.luong@vn.ey.com

## **EY | Building a better working world**

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

### **All in to shape the future with confidence.**

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

©2026 EY Law Vietnam Limited Liability Company. All Rights Reserved.

APAC No. 16011001

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

[ey.com/en\\_vn](https://ey.com/en_vn)