



Shape the future
with confidence

Legal - Forensics Newsletter

No.3 | September 2026

Visit other Updates [here](#).

Every whistleblowing investigation, at its core, is a personal data protection exercise

This Legal - Forensics Newsletter examines the key personal data protection issues that arise throughout the whistleblowing lifecycle and explores how organizations in Vietnam can balance confidentiality, investigative effectiveness and compliance with applicable data protection laws.

Whistleblowing programs are typically designed to encourage reporting, protect confidentiality and support effective investigations. However, every whistleblowing report also triggers a range of personal data processing activities involving whistleblowers, reported individuals, witnesses and other stakeholders. Every stage of a whistleblowing investigation may involve the collection, use, disclosure, transfer and retention of personal data relating to multiple individuals. As regulatory scrutiny over personal data protection continues to increase, organizations should ensure that their whistleblowing frameworks are designed not only to investigate allegations effectively, but also to comply with the requirements of the Personal Data Protection Law No. 91/2025/QH15 (PDPL) throughout the investigation lifecycle.

This Legal - Forensics Newsletter highlights:

- Why whistleblowing is also a personal data protection issue
- Key PDPL considerations throughout the investigation lifecycle
- Common privacy, evidentiary and regulatory risks arising from whistleblowing investigations
- Practical challenges in balancing confidentiality obligations and data protection requirements during investigations
- Practical measures to strengthen whistleblowing and data protection compliance

1. Overview

As discussed in our previous Legal - Forensic Newsletter No.1, [Whistleblowing in the global compliance landscape](#), a whistleblowing report rarely involves only the whistleblower and the individual concerned. In practice, a report may be reviewed by compliance personnel, HR, legal, internal audit, management, external advisers and, in some cases, regional or global investigation teams. As information moves across multiple stakeholders and functions, personal data is often collected, accessed, shared, retained and reviewed throughout the investigation lifecycle.

From a data protection perspective, whistleblowing arrangements therefore extend far beyond the operation of a reporting channel. A single report may contain personal data relating to multiple individuals, including the whistleblower, the reported person, witnesses and other third parties. It may also involve sensitive personal data, internal disclosures, cross-border transfers and long-term retention of investigation records.

As a result, organizations should view whistleblowing not only as an ethics and compliance mechanism, but also as an end-to-end personal data processing activity. Data protection considerations may arise at every stage of the whistleblowing lifecycle, from the initial collection of allegations and supporting evidence, through internal and external disclosures, to the retention, de-identification or deletion of investigation records. Organizations often focus on how to investigate a whistleblowing report; nonetheless, under the PDPL, an equally important question is whether the report can be lawfully collected, shared, used and retained in the first place.

2. Personal data protection throughout the whistleblowing lifecycle

Once a whistleblowing report is submitted, organizations may face different data protection considerations at each stage of the whistleblowing lifecycle.

a) Collection of personal data

In many jurisdictions, particularly within the EU, organizations commonly rely on the legitimate interests basis under Article 6(1)(f) General Data Protection Regulation (GDPR) when operating whistleblowing programs. Vietnam's PDPL adopts a different approach. Rather than providing a broad and standalone legitimate interests basis, the PDPL permits personal data processing without consent only in specific circumstances prescribed by law.

As a practical matter, organizations operating whistleblowing programs in Vietnam will often need to determine whether to rely on consent¹ or on one of the statutory exceptions to consent.²

■ Consent:

Where a consent-based approach is adopted, organizations should ensure that privacy notices and consent forms clearly describe whistleblowing-related processing activities, including the purposes of processing, categories of personal data involved, categories of recipients, investigation-related disclosures and any cross-border transfers.³

Consideration should also be given to allowing data subjects to provide consent in respect of specific processing purposes rather than through a single broad consent.⁴ In practice, however, a consent-based approach may present significant operational challenges. In the

¹ Articles 9 and 11.1 of PDPL

² Articles 19.1 of PDPL

³ Articles 9.2 of PDPL

⁴ Articles 9.4(a) of PDPL

context of whistleblowing programs, this may require organizations to separately address not only the operation of the whistleblowing mechanism itself, but also related activities that may arise from an investigation, such as disciplinary proceedings, recovery of damages, dispute resolution, regulatory reporting or other compliance measures. As a result, the practicality and sustainability of a consent-based model should be assessed in light of the structure of their whistleblowing program and the potential difficulty of obtaining valid consent for each relevant processing purpose.⁵

- **Non-consent legal basis:**

Where organizations seek to rely on a statutory exception, the legal basis should be carefully assessed and appropriately documented. For example, if processing is relied upon as necessary for the performance of an agreement with the data subject,⁶ consideration should be given to whether whistleblowing-related processing activities are expressly contemplated in the relevant employment agreement or other contractual arrangements.

Similarly, where reliance is placed on the protection of legitimate rights and interests or other consent exceptions under the PDPL,⁷ such exceptions should not be treated as automatically applicable merely because an internal investigation is involved. The intended processing activities, purposes and governance framework should be clearly reflected in relevant internal documentation, such as personal data processing policies, whistleblowing policies, codes of conduct, internal investigation procedures or other compliance documents. This may help demonstrate that the processing forms part of an established and legitimate compliance framework rather than an ad hoc investigative exercise.

Identifying a legal basis is only part of the compliance analysis. Under the PDPL, organizations processing personal data without consent must also establish appropriate oversight mechanisms, including documented procedures, allocation of responsibilities, risk assessments, compliance reviews and complaint-handling mechanisms.⁸ Accordingly, the key question is often not whether consent can be avoided, but whether the organization can demonstrate that the chosen legal basis is supported by adequate governance measures and implemented consistently in practice.

There is therefore no one-size-fits-all approach. The most appropriate approach will often depend on the design of the whistleblowing program, the categories of data subjects involved and the robustness of the organization's contractual and governance framework.

b) Transfer of personal data

Personal data collected through a whistleblowing program rarely remains with a single individual or function. As a whistleblowing report progresses through assessment, investigation and remediation stages, personal data may be shared with different stakeholders.

- **Internal transfers:**

Internal transfers commonly occur between the investigation team, the case owner or compliance officer, and supporting functions such as HR, legal and internal audit.

⁵ Articles 9.4(a) of PDPL

⁶ Articles 19.1(d) of PDPL

⁷ Articles 19.1(a) of PDPL

⁸ Articles 19.2 of PDPL

Depending on the nature of the allegation, access may also be provided to senior management or other internal stakeholders with a legitimate need to know.

Where personal data is shared between departments within the same organization for purposes consistent with the originally notified processing purposes, organizations should nevertheless establish appropriate controls over the sharing and use of such data. Effective internal sharing therefore depends on documented procedures, clearly allocated responsibilities and controls against unauthorized disclosure to third parties.⁹

- **External transfers:**

Whistleblowing-related personal data may also be shared with external recipients, including external legal counsel, forensics specialists, investigation service providers, whistleblowing platform operators, parent companies, regional compliance functions or other entities within a corporate group.

Such transfers raise additional compliance considerations. Under Vietnam's data protection framework, organizations engaging a third party to process personal data should ensure that an appropriate personal data transfer agreement is in place. Depending on the circumstances, the agreement may need to address matters such as the processing purposes, categories of personal data, processing activity time limits, rights and obligations of the parties, incident response obligations and others.¹⁰

Regardless of whether the transfer is internal or external, additional safeguards should be considered where sensitive personal data is involved. Organizations should implement appropriate measures to protect personal data during transfer, including physical security measures for storage and transmission devices, encryption, and anonymization or de-identification,¹¹ and ensure that data-sharing arrangements are mapped and documented before a report is received, rather than addressed on an ad hoc basis during an active investigation.

c) Cross-border transfer

Cross-border data flows deserve particular attention. Many multinational organizations rely on global headquarters, regional compliance teams, global whistleblowing platforms and cloud-based infrastructure to receive and investigate reports, which may result in whistleblowing-related personal data being accessed or processed outside Vietnam.

Importantly, cross-border transfers may occur even where the whistleblowing report is submitted locally, for example where access is granted to a global compliance team, regional investigation function or overseas headquarters.

Where such transfers occur, organizations may need to prepare and maintain a cross-border personal data transfer impact assessment dossier¹² and comply with other applicable transfer requirements under Vietnamese data protection laws. This may include implementing appropriate contractual, organizational and technical safeguards, ensuring transparency toward data subjects, allocating responsibilities between the transferring and receiving parties, and establishing controls over any onward transfers to third parties.¹³

⁹ Article 7.4 of Decree 356/2025/ND-CP

¹⁰ Article 7.1 of Decree 356/2025/ND-CP

¹¹ Article 7.2 of Decree 356/2025/ND-CP

¹² Article 20 of PDPL

¹³ Article 7.4 of Decree 356/2025/ND-CP

d) Retention of investigation records

The conclusion of an investigation does not necessarily mark the end of the associated data processing activities. Investigation reports, witness statements and supporting evidence may continue to be required for employment matters, internal disciplinary proceedings, litigation, regulatory inspections, anti-money laundering compliance, audit purposes or the defence of legal claims. Nonetheless, retention periods should not be assessed solely from an employment law perspective.

Organizations should avoid retaining whistleblowing records indefinitely. This may be difficult to reconcile with the storage limitation principle under the PDPL, which generally requires personal data to be retained only for as long as necessary to fulfil the processing purpose, as agreed with the data subject or as otherwise permitted by law.¹⁴ Importantly, Vietnamese law does not prescribe a fixed retention period for whistleblowing records. Accordingly, retention decisions should be based on a documented assessment of legal, regulatory and business needs on a case-by-case basis.

In practice, organizations may consider adopting a lifecycle-based retention framework. During the investigation stage, records containing identifying information, such as names, job titles, departments, IP addresses, interview records, recordings and supporting evidence, may need to be retained to support fact-finding and case assessment. Following the completion of the investigation, relevant records may continue to be retained for a reasonable period to address potential complaints, labor disputes, litigation, regulatory inquiries or newly emerged circumstances arising from the case. Depending on the nature of the allegations and the associated risks, organizations may determine that retention for a defined post-investigation period is necessary to protect their legitimate legal and compliance interests.

A clearly documented retention and deletion framework can help organizations demonstrate compliance with the PDPL while ensuring that whistleblowing records remain available for legitimate legal, regulatory and business purposes when required.

e) Security measures

Whistleblowing reports frequently contain sensitive personal data under the PDPL, particularly where they relate to health information, private-life information, disciplinary matters or internal investigations.¹⁵ In addition, particular attention should be paid to protecting the identity of whistleblowers and restricting access to information that could indirectly reveal their identity. A breach involving whistleblower identity may jeopardize the investigation itself, expose the organization to regulatory scrutiny and undermine confidence in the whistleblowing framework. Appropriate technical and organizational safeguards should therefore be implemented, proportionate to the sensitivity of the information involved.

In practice, this may include role-based access controls, confidentiality obligations, internal handling procedures,¹⁶ access logs and periodic access reviews. Access should be limited to individuals with a genuine need to know throughout the investigation lifecycle. Particular care should also be taken where information is shared with external advisers, platform providers, affiliates or overseas recipients, with appropriate contractual, organizational and security safeguards in place.

¹⁴ Article 14.1 of PDPL

¹⁵ Article 4.1 of Decree 356/2025/ND-CP

¹⁶ Article 4.2 of Decree 356/2025/ND-CP

Individually, each requirement may appear manageable. In practice, however, the most challenging situations often arise when confidentiality obligations, investigative objectives, labour law considerations and personal data protection requirements pull in different directions.

3. Risks and compliance challenges

a) Balancing confidentiality and transparency

A whistleblowing investigation often gives rise to a fundamental tension between two competing objectives. On the one hand, organizations must protect the confidentiality of whistleblowers, prevent retaliation and preserve the integrity of the investigation. On the other hand, individuals whose personal data is contained in a whistleblowing report may have legitimate expectations regarding how their personal data is collected, used and disclosed.

Vietnamese laws are silent on this matter. Looking up to more matured jurisdictions, the European Union (EU) faces the same challenge. Within the EU, the Whistleblower Protection Directive requires confidential reporting channels and protection against retaliation,¹⁷ while the GDPR separately regulates transparency and data subject rights. Neither regime automatically overrides the other. Instead, organizations are generally expected to strike an appropriate balance between protecting the investigation and respecting data protection rights.

In practice, this means that confidentiality should not be treated as a blanket justification for withholding information indefinitely. Organizations may consider adopting a phased notification approach, taking into account the individual's role in the investigation, the status of the investigation and the risk that disclosure could compromise fact-finding efforts or expose a whistleblower. Where notification is delayed or certain information is withheld, the rationale should be documented and periodically reviewed rather than applied automatically.

b) Privacy compliance and evidentiary risks

Organizations often focus on whether the evidence substantiates the allegation. Equally important, however, is whether the evidence was collected and processed lawfully.

Issues may arise where investigators access employee communications without an appropriate legal basis, collect information beyond the stated investigation purpose, or disclose evidence to persons who do not have a legitimate need to know. Such shortcomings may not only create separate privacy claims, but may also undermine the organization's position in subsequent disciplinary or employment or litigation proceedings.

This risk is particularly relevant under Vietnamese procedural laws. Under the 2015 Civil Procedure Code, evidence must be collected and submitted in accordance with statutory procedures, and specific requirements apply to the authenticity and origin of evidence, including electronic records, audio recordings and visual materials.¹⁸ As a result, organizations should not assume that information obtained during an investigation will automatically be accepted or carry the expected evidentiary weight in future proceedings.

The practical lesson is clear: in a whistleblowing investigation, the manner in which information is obtained and handled can be as important as the information itself. Whether a whistleblowing program relies on consent or a statutory exception under the PDPL, organizations should ensure that the collection and processing of personal data are supported by an appropriate legal basis and governance framework. Otherwise, even where

¹⁷ Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, Articles 9(1)(a), 16(1), 19 and 21(1)

¹⁸ Articles 93 and 95 of Civil Procedure Code No. 92/2015/QH13

misconduct is substantiated, questions may arise as to whether the information was lawfully obtained, used and disclosed, potentially undermining the organization's position in subsequent proceedings.

c) Regulatory and enforcement risks

Non-compliance with personal data protection requirements in whistleblowing investigations may expose organizations to significant regulatory risks under Decree No. 330/2026/ND-CP. Depending on the violation, organizations may face administrative fines of up to VND3 billion or 5% of the preceding year's revenue for certain cross-border data transfer violations.¹⁹ The risks extend beyond monetary penalties. Organizations may also be subject to additional sanctions, including the suspension of personal data processing activities, revocation of relevant licences or certificates, and confiscation of means used to commit the violation. Regulators may further require corrective actions, such as deleting unlawfully processed personal data, fulfilling data subject rights, notifying affected individuals, issuing public apologies or disgorging unlawful gains. In serious cases, personal data violations may also give rise to criminal liability.

4. Key recommendations

To strengthen the resilience of their whistleblowing framework, organizations should consider:

- **Reviewing the legal basis** for whistleblowing-related personal data processing and ensuring it is appropriately documented
- **Mapping data flows** across the investigation lifecycle, including internal sharing, external disclosures and cross-border transfers
- **Reviewing arrangements** with whistleblowing platform providers, cloud vendors and external advisors
- **Aligning policies and procedures** covering whistleblowing, personal data protection, investigations, evidence handling and information security
- **Establishing clear rules** on access control, retention, anonymization and deletion of investigation records
- **Assessing regulatory readiness** under the PDPL and Decree No. 330/2026/ND-CP, particularly for cross-border transfers, data subject rights and incident response

In an enforcement scenario, regulators may scrutinize not only the outcome of an investigation, but also every stage of how personal data was collected, shared, retained and secured. Organizations should therefore treat whistleblowing compliance and personal data protection compliance as two sides of the same process.

¹⁹ Article 7.4 Decree 330/2026/ND-CP
No.3 | September 2026



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



Saman Bandara | Senior Partner, Forensics & Forensic Technology Leader

Ernst & Young Vietnam Limited

saman.bandara@vn.ey.com



Hieu Duy Nguyen | Law Leader and Managing Director

EY Law Vietnam Limited Liability Company

hieu.d.nguyen@vn.ey.com



Thach Thi Cam Tran | Director

EY Law Vietnam Limited Liability Company

thach.cam.tran@vn.ey.com



Thuy Thu Nguyen | Manager

Ernst & Young Vietnam Limited

thuy.thu.nguyen2@vn.ey.com

Hanoi Office



Anh Thuy Pham | Associate Partner

EY Law Vietnam Limited Liability Company

anh.thuy.pham1@vn.ey.com



Linh Hoang Anh Nguyen | Director

EY Law Vietnam Limited Liability Company

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 | EY 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. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

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

APAC No. 16240901

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