Nhat Nam Law LLC (ATLAW)

Publication

A Practical Data Protection Checklist for Businesses in Vietnam

Law reviewed as at 24 October 2026.

Who this guide is for

This guide is intended for management, legal, HR, marketing and IT teams reviewing ordinary business processing of personal data in Vietnam. It offers a practical starting point under Personal Data Protection Law No. 91/2025/QH15 of 26 June 2025 and Decree No. 356/2025/ND-CP of 31 December 2025, both effective from 1 January 2026. It is not a sector-specific compliance manual or a certification of compliance. Decree 356 replaced Decree No. 13/2023/ND-CP from that date. [1–2]

The steps below distinguish statutory issues from suggested implementation measures. A company's obligations depend on its activities, role, data and any applicable exception. An English-language website or an overseas customer does not, by itself, establish that the GDPR applies. Any foreign-law analysis should be undertaken separately where its territorial or other application rules are met.

Contents

1. Identify the data and the processing activity
2. Determine the company's role and lawful route
3. Make consent and collection information workable
4. Review providers, recipients and overseas processing
5. Assess impact-file and personnel requirements
6. Build a rights-handling process
7. Set retention, security and incident procedures
8. Use the implementation checklist
9. Practical steps for businesses
10. Legal sources and references

1. Identify the data and the processing activity

Legal issue. The Law covers more than a customer database. Its definitions include collection, analysis, encryption, correction, deletion, disclosure, transfer and other processing. Article 3 requires processing within a specific, clear scope and purpose, with appropriate accuracy, retention and protective measures. Decree 356 distinguishes basic and sensitive personal data in Articles 3–4. [1–2]

Suggested implementation. Start with processes, not software names. Review recruitment, payroll, customer enquiries, supplier contacts, access control, newsletters and website interactions. For each process, identify the people concerned, the data collected, its source, purpose, systems, users and recipients. Ask why each field is

needed. A business contact's name and identifiable email should not be disregarded merely because the relationship is business-to-business.

Separate the classification of data from the company's estimate of commercial importance. HR health information, for example, calls for a sensitive-data assessment. Website technologies should also be examined for what they actually collect and transmit. The presence of a particular plugin is not a reliable substitute for a technical inventory.

2. Determine the company's role and lawful route

Legal issue. Article 2 distinguishes controllers, processors and parties that both determine and carry out processing. Article 9 addresses consent; Article 19 sets out cases where processing may occur without consent, subject to the applicable conditions and safeguards. Vietnamese law should be assessed on its own terms rather than importing a general “legitimate interests” basis from another jurisdiction. [1]

Suggested implementation. For each process, record who decides its purposes and means and who acts under instructions. Check the proposed route for collecting, using and disclosing the data. A service provider's contractual label should be compared with its actual activities. One organisation may have different roles in different processes.

Where relying on a statutory non-consent case, identify the relevant provision and explain why the facts fit. Keep this reasoning in the internal record. Where consent is required, design the collection journey to obtain and demonstrate it. A privacy policy should describe the actual processing; publishing one does not itself establish a lawful route for everything the business does.

3. Make consent and collection information workable

Legal issue. Article 9 requires voluntary, informed, clear and verifiable consent, with consent for each purpose and no treatment of silence as consent. It restricts making unrelated purposes a compulsory condition. Article 11 addresses consent before collection unless law provides otherwise. Decree 356, Article 6, requires evidence identifying the person, time and content of consent, prohibits default-consent mechanisms and requires sensitive-data notification where applicable. [1–2]

Suggested implementation. Distinguish responding to an enquiry from enrolling the sender in marketing. An optional newsletter choice should be explained separately from the contact form's immediate purpose. Keep the wording version and the relevant consent record together so that the business can demonstrate what the person agreed to at the time.

Review the actual interface rather than only its policy links. Test whether required and optional fields are understandable and whether the system records the choice accurately. Do not describe a withdrawal link, preference centre or cookie-rejection button unless that mechanism exists and works. A confirmation email can help evidence a subscription, but this guide does not present double opt-in as a universal statutory requirement.

4. Review providers, recipients and overseas processing

Legal issue. Data sharing and processing arrangements require assessment under Articles 17–20. Article 20's cross-border categories include specified overseas storage, transfers to overseas organisations or individuals, and the use of overseas platforms to process data collected in Vietnam. It contains impact-assessment requirements and exceptions, including a specific exception concerning an organisation's cloud storage of its own employees' data. That exception should not be extended automatically to unrelated customer or marketing processing. [1]

Suggested implementation. Ask providers where production data, backups and support access are located. Identify the relevant contracting entity and subcontractors. Review hosting, business email, payroll, customer-management systems, embedded maps, analytics and anti-spam services only where actually used.

An overseas brand name does not answer every transfer question; equally, a locally invoicing provider does not prove that all processing stays in Vietnam. Record the actual data flow and assess which requirements apply. Provider contracts should address instructions, permitted purposes, security, further recipients, rights assistance, incident escalation and deletion or return as appropriate. Assess the applicable transfer-agreement requirements under Decree 356, Article 7. [2]

5. Assess impact-file and personnel requirements

Legal issue. Articles 20–22 govern cross-border and processing impact assessments and updates. Article 21 distinguishes controller and processor obligations. The Law's Articles 38–39 and Decree 356, Article 41, contain specific exceptions and transition rules. Limited relief for certain small, start-up or micro businesses is not a general exemption from data protection law. Processing sensitive data, providing data-processing services or reaching the specified scale can affect eligibility. [1–2]

Suggested implementation. Determine whether an assessment file is required, who prepares and maintains it, the applicable submission event and deadline, and how changes will be tracked. Check any reliance on relief against the company's actual activities and size criteria. Do not assume that a low employee count is enough.

Review the applicable personnel or department requirements and the qualifications relevant to any external service. Keep business accountability clear even when work is outsourced. Where earlier files or consents exist, review Article 39 rather than assuming either that everything must be redone or that every historical arrangement can continue unchanged. [1]

Forthcoming procedural changes. Decree No. 392/2026/ND-CP was issued on 20 October 2026 and takes effect on 15 November 2026. Its Articles 42–47 amend specified Decree 356 procedures. Those amendments are not applied as current requirements in this guide; recheck the submission and assessment procedures before using it from that date. [3]

6. Build a rights-handling process

Legal issue. Article 4 identifies data-subject rights. Decree 356, Article 5, requires clear procedures and sets different response and implementation periods for specified requests. For example, qualifying withdrawal, restriction and objection requests carry a two-working-day response requirement and an ordinary 15-day implementation period, with qualifications including cases involving a processor or third party and permitted extensions. There is no single universal deadline that can safely replace the provision. [1–2]

Suggested implementation. Establish a monitored channel, an intake log, an identity-check procedure proportionate to the request and an escalation route. Record the request type, receipt, verification, legal assessment, applicable deadline, responsible team and outcome. Avoid routinely collecting a full identity-document copy when a less intrusive method can establish identity.

Test the process with a realistic example: a former subscriber asks to withdraw marketing consent and delete data. The team should distinguish stopping future newsletters from deciding whether other records have a lawful retention reason. Under Article 10, withdrawal does not retrospectively undo earlier processing. The response should explain the actual outcome and any lawful limits without promising deletion from every system instantly. [1]

7. Set retention, security and incident procedures

Legal issue. Article 3 ties retention to an appropriate period for the processing purpose unless law provides otherwise. Article 23 requires notification of specified violations capable of causing the stated harm no later than 72 hours after detection; it also requires processors to notify the relevant controller promptly. This should not be reduced to a claim that every technical event has the same reporting obligation. [1]

Suggested implementation. Adopt a retention schedule by record category, with a reason, trigger, responsible owner and deletion method. Distinguish statutory record-keeping from a business preference to keep information. Address backups and legal holds in a way the systems can actually implement.

Match controls to the risk: access permissions, account management, device protection, secure sharing and recovery arrangements are useful review topics. Avoid public promises of absolute security. For incidents, set an internal escalation period short enough to allow assessment and any external notice within the applicable deadline. Preserve the discovery time, affected data, likely consequences, containment actions and reporting decision.

8. Implementation checklist

The evidence suggestions below are practical tools; they are not all documents with prescribed statutory titles. Each item should be completed, marked not applicable with a reason, or assigned a remediation owner.

Review area	Evidence to prepare	Character
Purposes and data	Process inventory, necessary fields, basic/sensitive classification	Implements Articles 2–3 and Decree 356 Articles 3–4

Review area	Evidence to prepare	Character
Role and processing route	Role assessment and consent or statutory-exception analysis	Legal assessment under Articles 2, 9 and 19
Collection and consent	Collection wording, interface test and evidence of any required consent	Legal requirements; format depends on the process
Providers and recipients	Actual data-flow map, provider answers and relevant agreements	Legal assessment plus recommended evidence
Overseas processing	Location and access findings, applicable assessment or documented exception	Legal assessment under Article 20
Impact files and personnel	Applicability decision, current files, update register and responsible persons	Applicable legal requirements; no blanket SME exemption
Rights requests	Monitored channel, request log and request-specific deadline matrix	Implements Article 4 and Decree 356 Article 5
Retention and protection	Category schedule, permissions review and deletion evidence	Legal principles supported by operational controls
Incidents	Escalation procedure, discovery record and reporting assessment	Article 23 plus recommended readiness measures

9. Practical steps for businesses

Choose one high-exposure process and complete it from collection to deletion before attempting to rewrite every document. Use the findings to align the notice, consent journey, provider contract and internal instructions. Expand to other processes with the same evidence standard.

Set a management review date and track material changes, including new software, a different overseas recipient or a new use of existing data. Recheck the law before relying on an exemption or submitting an assessment file. An implemented process with a clear owner provides a more useful compliance foundation than a policy that describes controls the business has not adopted.

10. Legal sources and references

All sources accessed on **24 October 2026**. English descriptions are explanatory and are not represented as official translations.

1. Personal Data Protection Law No. 91/2025/QH15 of 26 June 2025, effective 1 January 2026; signed Vietnamese text. Relevant provisions: Articles 2–4, 9–11, 17–23 and 38–39.

2. Decree No. 356/2025/ND-CP of 31 December 2025, official Gazette text, effective 1 January 2026. Relevant provisions: Articles 3–7, 13–16, 41–42 and the applicable impact-assessment procedures and forms. Article 42 repeals Decree 13/2023 from 1 January 2026.

3. Decree No. 392/2026/ND-CP of 20 October 2026, Articles 42–48; signed text, particularly pages 31–34. Effective 15 November 2026; enacted but not yet effective at the research cut-off.

This publication provides general information based on sources reviewed as at 24 October 2026. It does not constitute legal advice on any specific matter. The application of Vietnamese law depends on the relevant facts and circumstances.