

PERSONAL DATA PROTECTION UNDER VIETNAMESE LAW

Know your obligations. Control the risks. Build trust.



COMPLYING WITH PERSONAL DATA LAW IN VIETNAM

PDP Law No. 91/2025/QH15 in force from 01/01/2026.

Penalties under Decree 330/2026/ND-CP from 19/08/2026.

Which businesses must comply?

If **ONE** of the signs below applies, your business processes personal data and falls under Law 91/2025/QH15.

	You have employees or job applicants · HR files, payroll, insurance, ID cards	☐
	You have individual customers · Names, phone numbers, emails, delivery addresses	☐
	You use CCTV or biometric time clocks · Fingerprints and faces are sensitive data	☐
	You use cloud, email, software or AI · Especially with servers located abroad	☐
	You send data to partners · Accounting, banks, insurers, logistics, agents	☐

Who must do what?

Type of business	Core obligations*	DPIA file, file updates, data protection staff
Medium & large firms, FDI	Mandatory	Mandatory
Any size if it processes sensitive data, or data of 100,000+ people, or provides data processing services	Mandatory	Mandatory, no exemption
Small enterprises, start-ups	Mandatory	Optional until 1 January 2031
Household & micro-businesses	Mandatory	Not required

*Core obligations: obtaining consent, honouring data subjects' rights, protection measures, breach notification within 72 hours.

01/01/2026

Law 91 and Decree 356 take effect

19/08/2026

Penalties under Decree 330 begin

VND 3 billion

General maximum fine for organisations (≈ USD 115,000)

Sources: Law 91/2025/QH15 Art. 1, 8, 38; Decree 356/2025/ND-CP Art. 4, 41; Decree 330/2026/ND-CP Art. 7, 80. Rate VND 26,100/USD.

Three things leaders must know

Personal data protection is now an enforceable obligation, and businesses must be able to prove what they have done.

1

Data is everywhere

Employee and customer records, CCTV and attendance logs are all personal data. Encrypted data is still personal data.

Law 91 Art. 2, 12.1

2

An operational issue

The law requires coordinated institutional, technical and people measures, not just work by the legal team.

Law 91 Art. 3.4

3

Evidence is required

DPIA files, consent logs, 72-hour breach notices. In a dispute, the business carries the burden of proof.

Law 91 Art. 21, 23; Decree 356 Art. 6.2

A data incident affects four areas of the business



Customers & employees

They may request access, correction, deletion or restriction, complain, sue and claim damages (Law 91 Art. 4).



Operations

Unannounced inspections; processing may be halted until files are filed (Decree 356 Art. 31; Decree 330 Art. 55).



Finance

Fines up to VND 3 bn, 5% of revenue (cross-border) or 10× proceeds (data trading), plus damages (Law 91 Art. 8).



Business opportunities

Data transfer and cloud contracts must include data protection clauses (Decree 356 Art. 7, 12).

+VND 17.5 bn
(≈ USD 670,000)

Average added cost of a breach at organisations with high levels of uncontrolled AI use (shadow AI). One in five surveyed organisations reported a shadow-AI-related incident.

Quick guide by role: CEO p. 2–3, 10, 13 · Legal p. 5–10 · HR p. 4, 8, 9 · IT p. 7, 11–12 · Quality, internal control p. 8, 9, 12, 13

Sources: IBM, *Cost of a Data Breach Report 2025* (converted at VND 26,100/USD); Law 91/2025/QH15; Decree 356/2025; Decree 330/2026.

Risks in everyday work

No hacker needed. A routine action can create a legal obligation.

ILLUSTRATIVE



Sending payroll to a partner

Data: Names, salaries, bank accounts, insurance

Risk

An unprotected Excel file is emailed, forwarded or kept too long by the partner; no data processing agreement is in place.

Questions to resolve

Is the partner a processor with a contract (Law 91 Art. 37.2)? Is the file protected in transfer (Decree 356 Art. 7)? Who deletes it afterwards?



Uploading customer files to an AI tool

Data: Contracts, ID cards, transaction history

Risk

A platform abroad may trigger a cross-border transfer; data is used beyond the notified purpose; the provider retains the data.

Questions to resolve

Which tools are approved? Is the data de-identified? Is a cross-border transfer file required (Law 91 Art. 20)?



Fingerprint or face time-keeping

Data: Biometric data (sensitive)

Risk

Staff are not told it is sensitive data; the device or vendor cloud is exposed; data is reused for other purposes.

Questions to resolve

Are employees clearly informed (Law 91 Art. 25.3)? Is there physical security and restricted access (Art. 31.4)? Is there a 72-hour incident process (Decree 356 Art. 29)?

Data risk does not only start with an attack. It arises when a business collects too much, shares without control, or does not know where its data is processed.

Obligations by sector and size

The law applies to every organisation. Exemptions cover only 3 documentation and staffing duties, not the whole law.

Sector	Typical activities	Data types	Responsible function
Manufacturing / FDI	Recruitment, attendance, CCTV, payroll	Identity, biometrics, bank accounts	HR, Admin, IT
Retail / e-commerce	Loyalty, delivery, advertising	Contacts, purchase behaviour, location	Marketing, Customer care
Finance, banking, insurance	Credit, payments, underwriting	Financial, credit (sensitive)	Compliance, Risk
Healthcare	Medical care, health insurance	Health (sensitive)	Medical records, IT
Education	Admissions, school records, classroom CCTV	Children's data	Academic affairs, Admin
Technology / Outsourcing	Operating systems for clients	Clients' data	Legal, CTO
Logistics / Travel	Shipping, bookings, visas	Passports, location, data sent abroad	Operations, Legal

What counts as sensitive personal data?

Health	Biometric, genetic	Bank accounts, transactions, credit
Location from positioning services	ID card images, e-ID passwords	Private life, family secrets
Political and religious views	Racial or ethnic origin	Behaviour on social media and online services

Sector notes

Finance and banking: annual compliance assessment, logging of all processing, sensitive-data incident reports within 72 hours (Decree 356 Art. 8).

Children aged 7 and over: both the child and the legal guardian must consent before private information is disclosed (Law 91 Art. 24).

Sources: Law 91/2025/QH15 Art. 1, 24, 38; Decree 356/2025/ND-CP Art. 4, 8, 41.

The legal framework

Three layers: core obligations, activity-specific requirements and sanctions.

1 CORE OBLIGATIONS

Law on Personal Data Protection 91/2025/QH15	01/01/2026	Principles, rights, consent, DPIA, cross-border transfer, breach notification
Decree 356/2025/ND-CP (replaces Decree 13/2023)	01/01/2026	Sensitive data list, request deadlines, files, staffing, services

2 ACTIVITY-SPECIFIC REQUIREMENTS

Law on Data 60/2024/QH15 + Decree 165/2025/ND-CP	01/07/2025	Core and important data; encryption; cross-border transfer
Law on Cybersecurity 116/2025/QH15 + Decrees 331, 333/2026	01/07/2026; 19/08/2026	Information system protection by security level
Decree 341/2026/ND-CP (civil cryptography)	01/09/2026	When trading or using encryption products
Law on Artificial Intelligence 134/2025/QH15 + Decree 142/2026 + Decision 33/2026/QD-TTg	01/03/2026; 15/08/2026	Risk classification, transparency, high-risk AI list
Law on E-Transactions 20/2023; Law on Consumer Protection 19/2023; labour and sector laws	—	Depending on the activity

3 SANCTIONS

Law 91 Art. 8 + Decree 330/2026/ND-CP (penalties in cybersecurity and personal data protection)	19/08/2026	Fines per violation, remedial measures
---	------------	--

Overlap: a DPIA and cross-border transfer file made under Law 91 replace the risk assessments required by the data law, including for core or important data that is personal data (Law 91 Art. 5.4; Decree 356 Art. 42.3).

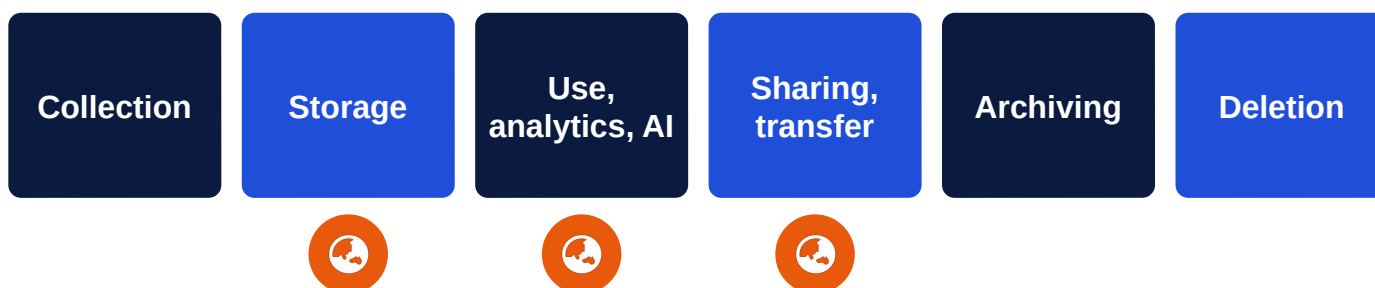
Sources: original legal texts; effective dates checked against each text's effectiveness clause.

Roles and data flows

Identifying roles comes first, because obligations follow roles.

Role	Short definition	Example
Controller	Decides the purpose and means of processing	A company outsourcing its payroll
Processor	Processes on the controller's instructions under a contract	Payroll service firm, cloud provider
Controller-processor	Both decides and processes directly	A company running its own hiring and HR
Third party	Another party involved in processing as permitted by law	Auditor, insurer

Data lifecycle: who receives it, where is it processed?



Orange icon: stages that may involve cross-border transfer

Three cases that count as cross-border transfer

a) Moving data stored in Vietnam to storage systems abroad

b) Sending data to organisations or individuals abroad

c) Using an overseas platform to process data collected in Vietnam

Two common mistakes: (1) Encryption does not stop data being personal data. (2) Only de-identified data, which can no longer identify a specific person, ceases to be personal data.

Sources: Law 91/2025/QH15 Art. 2, 12.1, 20.1.

Lawful basis and individual rights

Every processing activity needs a basis, and every data subject request must be handled on time.

What to do	Evidence needed	Reference
Set a specific purpose for each activity; collect only necessary data	Register of processing activities (recommended)	Law 91 Art. 3.2
Obtain consent per purpose; no pre-ticked consent; silence is not consent; state clearly when data is sensitive	Verifiable consent log: who, when, what	Law 91 Art. 9; Decree 356 Art. 6
Where consent is not required, set up oversight	Basis analysis; procedures; periodic review	Law 91 Art. 19
Receive and handle data subject requests	Procedure, forms, deadline tracker	Decree 356 Art. 5
Keep data only as long as allowed; delete unsuccessful applicants' files; delete leavers' data (unless agreed or required by law)	Retention policy; deletion records	Law 91 Art. 14, 25

Deadlines for data subject requests

Every request: respond within 2 working days, then complete within the deadlines below

Request type	Done by the business	When a processor must act	One extension, maximum
Withdraw consent, restrict, object	15 days	20 days	15 days
Access, correct, provide	10 days	15 days	10 days
Delete data	20 days	30 days	20 days

Sources: Law 91/2025/QH15; Decree 356/2025/ND-CP Art. 5, 6. No consent, or consent cannot be proven: fine of VND 30–50 million (Decree 330 Art. 43).

Files, staff and vendors

Documentation duties are conditional. Know when they apply, who does them and where to file.

Obligation	Applies when	Key requirements
Data protection impact assessment (DPIA)	The business is a controller; processors prepare one as agreed	File one original within 60 days of starting processing; update every 6 months if changed, within 10 days after restructuring (Law 91 Art. 21–22; Decree 356 Art. 19–20)
Cross-border transfer impact assessment (DTIA)	Any of the 3 cases on page 7	File within 60 days of the first transfer, with contract, data flow map and recipient assessment (Decree 356 Art. 18)
No DTIA required	Exempt cases	Storing employee data in the cloud; cross-border HR under labour rules; contracts, shipping, payments, hotels, visas (Law 91 Art. 20.6; Decree 356 Art. 17.3)
Data protection officer or unit	All organisations, except those exempt on page 2	Appointed in writing; college degree or higher, at least 2 years' experience, trained; may be outsourced (Decree 356 Art. 13, 15–16)
Data transfer contract	When data is transferred to another party	7 elements: purpose, data types, duration and deletion, legal basis, protection duties, data subject rights, cooperation on breaches (Decree 356 Art. 7.1)
Cloud service contract	When cloud services process personal data	Specify data flows, roles and security measures; data must be encrypted at rest and in transit (Decree 356 Art. 12)
Data processing service certificate	When the business processes data on behalf of clients as a service	Issued by the Ministry of Public Security; 9 service types, incl. operating systems for clients and personal data encryption (Decree 356 Art. 21–25)

Transition: consents and files submitted under Decree 13/2023 before 1 January 2026 remain valid; updates follow the new rules (Law 91 Art. 39).

Sources: Law 91/2025/QH15; Decree 356/2025/ND-CP.

Penalties for non-compliance

Maximum fines are ceilings, not typical amounts. Operational consequences often come before the fine.

VND 3 billion

≈ USD 115,000
Ceiling for general violations

5% revenue

of the preceding year
Cross-border transfer violations

10 times

the proceeds
Buying or selling personal data

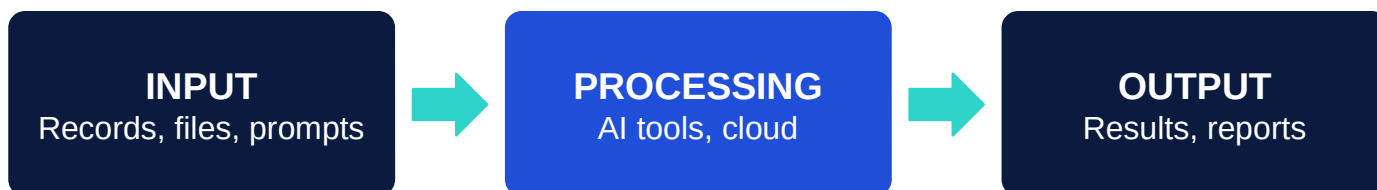
Violation (organisation)	Fine (VND)	Decree 330
Processing without consent; pre-ticked consent; no consent log	30–50 million	Art. 43.1
Treating silence as consent; continuing after a request to stop	50–70 million	Art. 43.2
No DPIA prepared or filed within 60 days (processing may be suspended until filed)	20–30 million	Art. 55.1, 55.3
Reporting a harmful breach to the authority later than 72 hours	40–60 million	Art. 54.3
No data protection officer, or an unqualified one	20–30 million	Art. 57.2
Monitoring software or CCTV without telling employees; not deleting leavers' data	50–70 million	Art. 61.2
Using cloud without encrypting customer data at rest and in transit	50–70 million	Art. 69.2
Biometric data without physical security, access limits or 72-hour notice	50–70 million	Art. 70.1
Cross-border transfer without a file, leading to a leak of 10,000+ people's data	1–5% of Vietnam revenue	Art. 56.3; transfers suspended 6–12 months

Ceilings apply to organisations; individuals face up to half (Law 91 Art. 8; Decree 330 Art. 7). Beyond fines: forced deletion of unlawfully collected data, return of proceeds, damages, possible criminal liability.

Specific obligations depend on the processing activity, role, data type and applicable conditions. Define your scope before choosing files and solutions.

Using AI and cloud under control

AI is not banned. What matters is knowing what data goes in, where it is processed and how results are used.



1 Approved tools
Which tools are used? Where are the servers? Is a cross-border transfer file required? *Law 91 Art. 20.1*

2 Input data
Limit sensitive data; de-identify or anonymise before input. *Law 91 Art. 30.1; Decree 356 Art. 9.3*

3 Vendors and subcontractors
Are inputs stored? Used for training? Where are logs kept? *Decree 356 Art. 12*

4 Outputs
AI inferences that identify a person are personal data. Automated processing requires notice, explanation and an opt-out. *Decree 356 Art. 10*

5 Retention and deletion
When are inputs, history and uploaded files deleted? *Law 91 Art. 14*

Under the new AI and cloud rules

AI and cloud systems need security, authentication and access control (Law 91 Art. 30.3). Personal data in the cloud must be encrypted at rest and in transit (Decree 356 Art. 12.4). AI deployers inherit the provider's risk classification and must reclassify if changes create new risks (Law 134/2025 Art. 10.2); high-risk systems follow a separate timeline (Decision 33/2026/QD-TTg).

Sources: Law 91/2025/QH15; Decree 356/2025/ND-CP; Law 134/2025/QH15; Decision 33/2026/QD-TTg.

Three pillars of data protection

No pillar stands alone. Without one, the other two lose their effect.

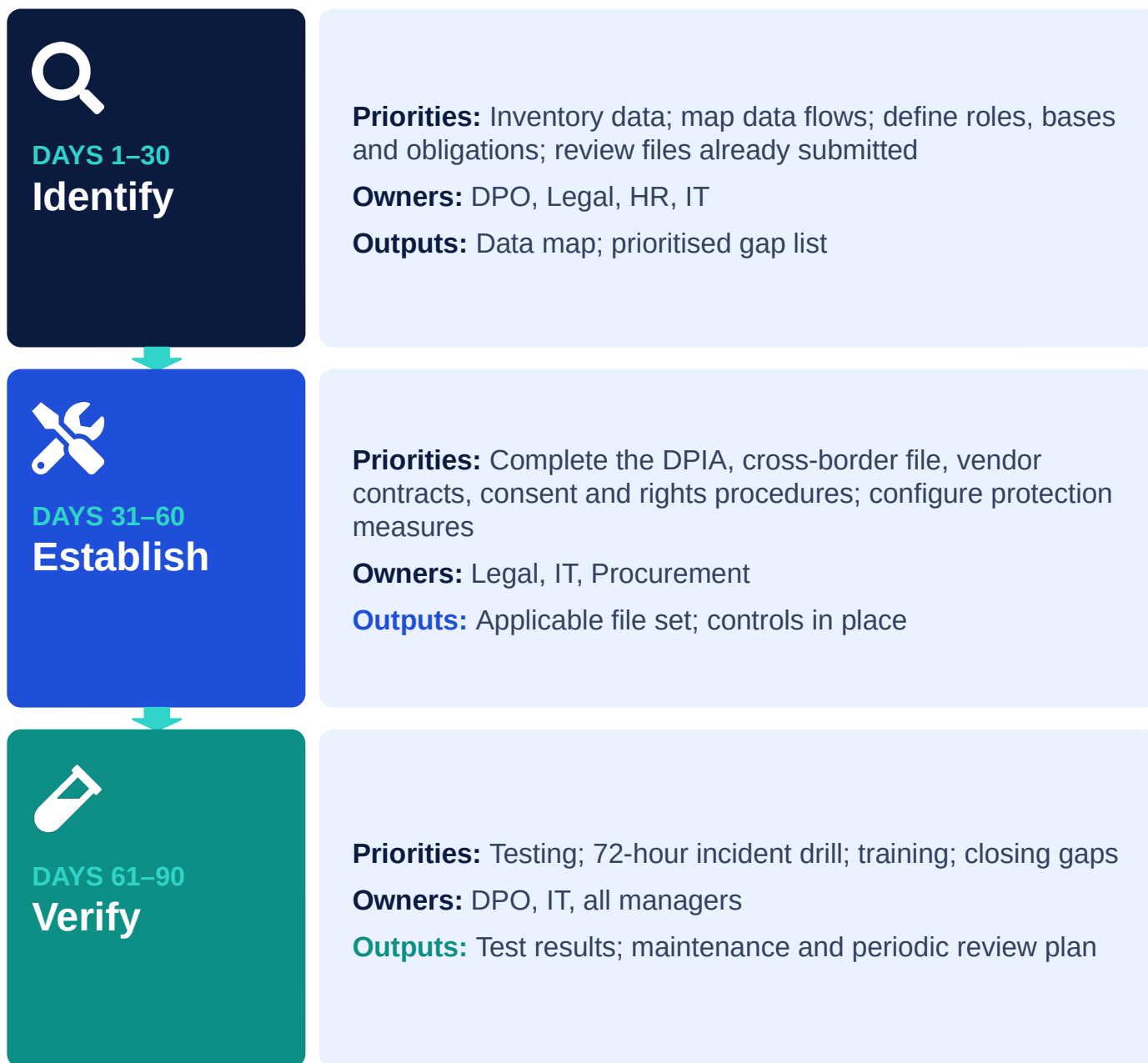
 PROCESS	 PEOPLE	 TECHNOLOGY
Register of processing and lawful bases RECOMMENDED	Appoint a data protection officer or unit (Law 91 Art. 33.2) MANDATORY	Role-based access to sensitive data (Decree 356 Art. 4.2) MANDATORY
Policy, notices, consent procedure (Law 91 Art. 9) MANDATORY	Assign responsibilities to each function RECOMMENDED	Multi-factor authentication for big data processing (Decree 356 Art. 9.3) MANDATORY IF APPLICABLE
Data subject rights procedure (Decree 356 Art. 5) MANDATORY	Regular training (Decree 356 Art. 9.2, 14) MANDATORY IF APPLICABLE	Encryption and key management (Decree 356 Art. 7.2, 12.4) MANDATORY IF APPLICABLE
Vendor contracts (Decree 356 Art. 7, 12) MANDATORY	Confidentiality agreements RECOMMENDED	Logging and access monitoring (Decree 356 Art. 8.1, 9.3) MANDATORY IF APPLICABLE
Incident response, 72-hour notice (Law 91 Art. 23; Decree 356 Art. 28) MANDATORY	Stop insiders sharing data with third parties (Decree 356 Art. 7.4) MANDATORY	Backup, recovery; secure deletion (Law 91 Art. 14.3) MANDATORY

Orange box: Decree 356 requires measures against unauthorised sharing by insiders. Here, process and people need an extra layer of control on the data files themselves.

Sources: Law 91/2025/QH15; Decree 356/2025/ND-CP. "Mandatory if applicable": when the business falls within the case the provision describes.

A 90-day foundation roadmap

Start by knowing what data you hold, then move on to files and tools.



Note: this roadmap is a recommended way to organise the work; it does not replace or extend legal deadlines. If a mandatory file is overdue (e.g. the 60-day DPIA), address it in phase 1 and seek legal advice.

Sources: AISA governance recommendations; filing deadlines per Law 91/2025/QH15 Art. 20, 21.

Have you identified all your data protection gaps?

Take a 10-minute survey for an initial review of governance, documentation and technical measures. The results show what to prioritise and prepare you for an expert discussion.



Scan the QR code to start
aisa.vn/assessment/pdp

After the survey: talk with AISA about your data protection needs and see a DCS demo in AISA's environment, using simulated data.

The survey relies on self-reported information and does not replace a legal assessment or system audit.



AISA · AI | Security | Automation

Developer of DCS, a Data-Centric Security solution in Vietnam.

Hotline: +84 905 885 539 **Email:** info@aisa.vn **Web:** aisa.vn

Address: 16th Floor, Saigon Tower, 29 Le Duan, Saigon, Ho Chi Minh City

This paper summarises Vietnamese law in force as of 15 October 2026 for reference only and is not legal advice. Seek professional legal advice for specific cases.