

Personal Data Protection Policy

Version 0.99 · 7 October 2026

Company	Pride Legal Co., Ltd. (บริษัท ไพร์ด ลีเกิ้ล จำกัด), registration no. 0105569087213
Version	0.99, an interim version published until version 1.0 is issued
Effective	7 October 2026
Owner	Data Protection Officer: Tanik Tangburanakij
Review	Every December, and whenever a system, a processor or the law changes
Contents	The rules for Pride Legal and its staff. The Privacy Notice for clients and website users is published at pridelegal.co.th/privacy and remains in force.

1. Purpose and scope

- 1.1 This policy states how Pride Legal collects, uses, discloses, keeps and deletes personal data under the Personal Data Protection Act B.E. 2562 (2019) (the “PDPA”). It binds every staff member and every processor that handles personal data for Pride Legal.
- 1.2 It covers the personal data of clients and their partners; prospective clients and people who contact Pride Legal through the website, ELSA, WhatsApp or e-mail; referral partners and their contacts; translators, witnesses, couriers and other suppliers; staff members and job applicants; and people photographed or recorded for Pride Legal’s channels.
- 1.3 Pride Legal is the data controller of that personal data. Where Pride Legal processes personal data on the written instructions of another business — for example a hotel that sells the service under its own name — Pride Legal acts as that business’s processor and follows its instructions as well as this policy.
- 1.4 The privacy documents work as one set: this policy states the rules; the Privacy Notice for clients and website users and the Privacy Notice for staff members and job applicants state what Pride Legal tells the people whose data it holds; the separate Consent Forms record what those people agree to. Until version 1.0 of this



policy is issued, where the Privacy Notice published at pridelegal.co.th/privacy differs from this policy, the Privacy Notice applies.

- 1.5 **Staff member** means the Director, every employee (including an employee on probation) and every intern. **Processor** means a person or business that processes personal data on Pride Legal's behalf and on its instructions.

2. Responsibilities

- 2.1 **The Director** is accountable for compliance, approves this policy, approves every processor and every new use of personal data, and provides the resources the rules require.
- 2.2 **The Data Protection Officer** is Tanik Tangburanakij, reachable at help@pridelegal.co.th and +66 64 959 0676. The Data Protection Officer advises staff, monitors compliance, keeps the record of processing (clause 14), handles requests (clause 12) and breaches (clause 13), and deals with the Office of the Personal Data Protection Committee. Because the core activity of Pride Legal is processing data that it treats as sensitive personal data (clause 5.1), Pride Legal appoints the Data Protection Officer under section 41(3) of the PDPA, which sets no minimum size, and gives the Officer's contact details to the Office of the Personal Data Protection Committee.
- 2.3 **Every staff member** handles only the personal data needed for the matters assigned to them, follows clauses 5 to 9, and reports any breach at once under clause 13.

3. Principles

- 3.1 Pride Legal collects only the personal data that a stated purpose needs, tells people what it collects and why at or before collection, uses the data only for that purpose or a purpose compatible with it, keeps it accurate, keeps it no longer than clause 8 allows, protects it under clause 9, and keeps records that show it has done so.
- 3.2 A new purpose requires a new notice and, where consent is the basis, a new consent before the data is used for it.



4. Lawful basis

4.1 Pride Legal processes personal data only on one of the bases below (sections 24 and 26 of the PDPA).

Processing	Basis
Preparing and delivering the marriage registration service: documents, translation, legalization, appointments, registration, the certificate, and coordination with the home country and the destination country	Contract with the client; explicit consent for sensitive data (clause 5)
Answering an enquiry before any contract (ELSA, the planner, WhatsApp, e-mail)	Steps taken at the person's request before a contract; explicit consent for sensitive data
Payments, invoices, accounting and tax	Legal obligation, and contract
Dealing with complaints, disputes and legal claims	Legitimate interest; for sensitive data, the legal-claims exception
Securing the website and measuring its use and its advertising	Legitimate interest
Sending updates and offers	Consent
Photographs, video and testimonials on Pride Legal's channels	Consent (explicit where the material reveals sensitive data)
Confirming a booking to the referral partner that introduced the client	Consent
Employment, payroll, tax and social security	Contract and legal obligation; for health data, the employment and social-security exception

4.2 Legitimate interest is relied on only after the Data Protection Officer has recorded, in the record of processing, why the interest is not overridden by the rights of the people concerned (a legitimate interest assessment, which the PDPC's guidelines recommend).

5. Sensitive personal data

5.1 In this business, sensitive personal data means above all data that reveals a client's sexual orientation, because a same-sex marriage record reveals it. Section 26 of the PDPA lists "sexual behaviour" among sensitive personal data, and neither the Act nor the Personal Data Protection Committee has said whether data that reveals sexual orientation falls within it; Pride Legal applies the stricter reading and treats that data as sensitive personal data. It also includes religion, race or ethnicity shown in passports or civil-status documents, health data (for example a staff member's medical certificate), and criminal-record data where a country requires a police certificate.



- 5.2 Pride Legal collects sensitive personal data only with the person's explicit consent (Consent Form A, or the consent step in the planner and ELSA), or where another exception in section 26 applies. Each partner in a couple gives consent for themselves; one partner cannot consent for the other.
- 5.3 Sensitive personal data is seen only by the staff assigned to the matter; is never used in marketing without a separate consent (Consent Form B); and is never disclosed to anyone — including a family member, an employer or a partner business — without the person's consent or a legal duty.
- 5.4 **Clients from states that criminalise same-sex relations.** Pride Legal sends no data to the home state's authorities unless the client has chosen that document route in writing; contacts the client only through the channel the client chose; and tells the client, before the registration, that the Thai marriage register is not public but that relatives such as parents may qualify as interested persons entitled to see or copy it.

6. Notices and consent

- 6.1 Pride Legal gives a notice at or before collection: the Privacy Notice to clients, prospective clients and website users (published at pridelegal.co.th/privacy, shown at account creation and at the consent step in ELSA, and linked in the first reply on WhatsApp and e-mail); the staff Privacy Notice to staff members and job applicants; and the text of Consent Form B to people photographed or recorded.
- 6.2 Consent is asked for in writing or electronically, separately from any other terms, in plain words, one item per purpose. Consent is never placed inside the Service Agreement and is never made a condition of the service for data the service does not need (section 19 of the PDPA).
- 6.3 For every consent, Pride Legal records who gave it, which items, the version of the text, the date and time, and how it was given (a signed form or a tick in the portal). A withdrawal is recorded the same way and acted on within seven days.
- 6.4 The second partner in a couple has no portal account. That partner gives consent on a signed Consent Form A or through a consent link sent to that partner's own e-mail address.

7. Handling rules for staff

- 7.1 **Company channels only.** Client personal data is received and kept only in the company systems: the client portal, Elsa, the office server, the company Microsoft 365 accounts and the company WhatsApp Business number. No staff member uses a personal WhatsApp or LINE account, a personal e-mail address or personal cloud storage for client data.



- 7.2 **Devices.** Staff use devices administered by Pride Legal, locked when unattended. A document downloaded to a device for a task is deleted from the device once the task is done.
- 7.3 **AI tools.** Client personal data is entered only into AI tools that the Director has approved under a data processing agreement, and never into a personal or free AI account.
- 7.4 **Original documents.** An original document received from a client is logged on receipt, kept in the locked cabinet, and returned against the client's signature as soon as the step that needs it is complete.
- 7.5 **Paper.** Documents are printed only where an office requires paper; copies no longer needed are shredded.
- 7.6 **Sharing.** Personal data is disclosed only to the recipients named in the notices, and only what that recipient needs. A copy of a passport or a civil-status document is never sent to a hotel, a planner or any other partner.
- 7.7 **Photographs.** Clients are photographed only with Consent Form B. Officials and other members of the public are not photographed.



8. Retention and deletion

8.1 Pride Legal keeps personal data for the periods below and then deletes it or makes it anonymous, so that no person can be identified from it.

Data	Kept for
Client matter record: names, contact details, the service, dates, advice given, the outcome, correspondence, consent records	10 years after the matter closes (the general limitation period, Civil and Commercial Code s.193/30)
Copies of identity and civil-status documents, translations and relationship evidence	1 year after the matter closes, for certificate, legalization and immigration work that follows the registration; longer only at the client's written request or while a claim is pending
Invoices, receipts and accounting records	5 years from the date the accounts are closed, or up to 7 years where the Director-General requires (Accounting Act B.E. 2543 s.14; Revenue Code s.87/3)
Enquiries that did not become a matter: ELSA conversations, planner answers, WhatsApp and e-mail enquiries	2 years after the last contact
Website visitor and advertising-measurement records	2 years after the last visit
Marketing list	Until consent is withdrawn
Photographs, video and testimonials	Until consent is withdrawn; removed from Pride Legal's own channels within 30 days of withdrawal
Staff personnel file	10 years after employment ends
Applications of candidates not hired	6 months after the decision, or 1 year with the candidate's consent
Supplier and partner records	10 years after the relationship ends
Rights Request Log and Breach Log	At least 2 years after the entry is closed (PDPC Notification on access requests B.E. 2569)
Backups	Deleted data leaves the backups when the backup cycle overwrites them

8.2 Deletion runs automatically where the system supports it. Where it does not, the Data Protection Officer carries it out at the December review and records it.

9. Security

9.1 **Organisational measures.** Access is given by role and only for assigned matters; access is removed on the day a person leaves; every employment contract carries a confidentiality duty; staff are trained under clause 15.



- 9.2 **Technical measures.** Client records are kept on Pride Legal's own server in Thailand, whose disk is fully encrypted; the server accepts no connection from the open internet, and staff reach it only through an encrypted private network; the application cannot delete records and every change is logged; records are backed up every night in encrypted form; card payments are handled by Stripe, so card numbers never reach Pride Legal; location data is removed from uploaded photographs. These measures follow the PDPC Notification on Security Measures B.E. 2565 (2022).
- 9.3 **Physical measures.** Original documents are kept in a locked cabinet in the office, in a building with controlled entry.

10. Processors and other recipients

- 10.1 A processor is engaged only with the Director's approval and under a written data processing agreement that limits it to Pride Legal's instructions, requires security and confidentiality, and requires it to report a breach to Pride Legal within 72 hours, and requires it to return or delete the data at the end (section 40 of the PDPA). The providers in use on the date of this policy are listed below. Where a provider also uses data for its own purposes — the advertising platforms and Stripe — it does so as a separate controller under its own terms.

Provider	Purpose
Microsoft (Microsoft 365, Entra ID, Clarity)	Staff e-mail, documents and accounts; website session analytics
Supabase	Website accounts, the client portal, enquiry and analytics records
Vercel	Website hosting and visit analytics
Stripe	Card payments
Anthropic	The ELSA website assistant and drafting tools
Meta (WhatsApp Business)	Client messaging
Google, Meta and TikTok	Advertising measurement
Tailscale	The private network to the office server
Certified translators and couriers	Translation and document transport in Thailand

- 10.2 District offices, the Ministry of Foreign Affairs, embassies and consulates, courts and other authorities receive personal data under their own legal powers; they are recipients, not processors.



11. Transfers outside Thailand

- 11.1 Personal data leaves Thailand when it is sent to a client's embassy or home authorities, when it is stored by a processor in clause 10 that holds data abroad, and when a client asks Pride Legal to engage a partner in another country.
- 11.2 Pride Legal transfers personal data abroad only on a ground the PDPA allows: that the transfer is needed to perform the contract with the client or steps the client asked for; that the processor applies safeguards recognised by the Personal Data Protection Committee, such as the ASEAN Model Contractual Clauses or the EU standard contractual clauses; or, where no other ground applies, the person's consent given after being told that the destination may not protect the data to the Thai standard (sections 28 and 29 of the PDPA, and the two PDPC notifications on transfers abroad B.E. 2566, in force since 24 March 2024).

12. Requests from the people whose data Pride Legal holds

- 12.1 Every person may ask for access to and a copy of their data, for its transfer to them or to another controller, for its correction, deletion or restriction, may object to its use, may withdraw consent, and may complain to the expert committee of the Personal Data Protection Committee (sections 19, 30 to 36 and 73 of the PDPA).
- 12.2 Pride Legal accepts a request in person, by post or by e-mail. A staff member who receives one passes it to the Data Protection Officer the same day. The Data Protection Officer records it in the Rights Request Log, confirms the person's identity within 15 days from contact details already held (asking for a new identity document only where there is no other way), and answers within 30 days of receipt, free of charge; the period is extended by at most 30 days, and only with written reasons given to the person (section 30 of the PDPA and the PDPC Notification on access requests B.E. 2569 (2026)). A refused request is answered with the reason and with the person's right to complain, and the refusal is entered in the record of processing.
- 12.3 A person may use Consent Form C, but no form is required.

13. Personal data breaches

- 13.1 A breach is any event in which personal data is lost, or is accessed, used, changed or disclosed without authority: a lost telephone, an e-mail sent to the wrong person, a document uploaded to the wrong client's portal, or an account taken over by another person.
- 13.2 A staff member who learns of a breach, or suspects one, telephones the Data Protection Officer at once.



- 13.3 The Data Protection Officer contains the breach, assesses the risk, notifies the Office of the Personal Data Protection Committee without delay and, where feasible, within 72 hours of Pride Legal becoming aware of it, unless it is unlikely to create a risk to the people concerned, and notifies those people without delay, with the steps they can take, where the risk is high (section 37(4) of the PDPA and the PDPC Notification on breach notification B.E. 2565 (2022)). Every breach is entered in the Breach Log, including one that was not notified.
- 13.4 A breach that involves client documents or data that reveals sexual orientation is treated as high risk.

14. Record of processing

- 14.1 The Data Protection Officer keeps a record of every processing activity — its purpose, the data and the people concerned, the basis, the recipients, any transfer abroad, the retention period and the security measures — in the company SharePoint, and updates it whenever a system or a processor is added (section 39 of the PDPA). The small-business exemption does not apply to Pride Legal, because its processing is not occasional, involves sensitive personal data, and requires a Data Protection Officer.

15. Training and discipline

- 15.1 Every staff member reads this policy within the first week of starting work and every December, and signs the acknowledgment in the Work Rules.
- 15.2 A breach of this policy is a disciplinary matter under the Work Rules. Deliberate disclosure of a client's sensitive personal data is a serious case for which the Work Rules do not require a prior warning.

16. Review

- 16.1 The Data Protection Officer reviews this policy, the record of processing, the Rights Request Log and the Breach Log every December. A change produces a new version; a significant change to a Privacy Notice is announced to the people concerned and, where consent is the basis, consent is asked for again.



17. Approval

17.1 This policy takes effect on the date of the Director's signature below.

For Pride Legal Co., Ltd.

Signed: Tanik Tangburanakij

Tanik Tangburanakij

Director and Data Protection Officer · 7 October 2026