



Privacy Notice - Employees

Document Code PIMS-AN-002 | Version 02

Effective Date 19 October 2026

Document Code	PIMS-AN-002
Document Title	Privacy Notice - Employees
Version	02
Effective Date	19 October 2026
Prepared By	Data Protection Officer (DPO)
Reviewed By	Managing Director (MD)
Approved By	Managing Director (MD)
Classification	Public
Reference Standard	ISO/IEC 27701:2025; Personal Data Protection Act B.E. 2562 (2019)

Document Revision History

Version	Date	Description of Change	Prepared – Reviewed – Approved
01	21 September 2026	Initial release	PIMS Working Team – MD – MD



02	19 October 2026	– Corporate document format applied (TH SarabunPSK, cover metadata, revision history, table of contents, approval block) – Content rebuilt from the ROPA: employee processing activities with personal data, purpose, lawful basis, recipients, transfers and retention – Lawful bases corrected (legitimate interests s.24(5), legal obligation s.24(6), social security health data s.26(5)(c)) – Removed: monitoring table with purposes and limits on use (sign-in logs not used to track working hours, endpoint telemetry not used for performance assessment, session logs reviewed by another person), endpoint telemetry and customer system session logs, and the statement that objecting to monitoring does not affect employment – Blank contact and retention fields completed; pre-publication instruction note removed – Merged with the 2022 Employee Privacy Notice (Notion), keeping the broader scope; notice also applies to personnel (interns, trainees and contract staff) – Personnel Administration and Group Health Insurance: additional personal data and purposes (e.g. emergency contact details, job application form, time attendance, military status, driving licence, vehicle registration, annual health checks, insured family members) – New activities: Payroll, Compensation and Welfare Benefits; Work Permit and Visa (foreign employees); Business Travel (domestic and overseas – passport, visa, emergency contact); Monitoring of IT Resources and Electronic Communications	DPO – MD – MD
----	-----------------	---	---------------



		– Sensitive data: health check results, blood group and disability; criminal record (work permit and visa) – Added: sources of personal data, personal data of other persons, new purposes, right to be informed, effect of consent withdrawal, longer retention where required by law – Recipients regrouped by category with duplicates merged (IT and cloud service providers, payroll and accounting service providers, banks, insurance and healthcare, government agencies) and extended (legal advisers, travel and event providers, affiliates, authorities, restructuring or merger); cross-border transfers extended to PDPA Section 28 exceptions (business travel) – Contact telephone changed to 02-105-3296 and added to Your rights – New activity Submission of Personnel Profiles to Customers (profile/CV, education history, certifications) with customers and prospective customers added as recipients – New activity Use of Employee Photographs and Videos in Social Media, Advertising and Marketing (consent, withdrawable at any time); social media platforms added as recipients and to transfers outside Thailand – Cross-border transfer wording aligned with PDPA Sections 28 and 29 and PIMS-PL-001 (adequacy, safeguards such as providers' data processing terms with standard contractual clauses, or Section 28 exceptions) – New activity Post-hire Criminal Record Check (all employees; explicit consent on form PIMS-FM-001-B Section 2; certificate kept in the HR employee file for the personnel-file retention period); notice extended to family members	
--	--	--	--



Version	Date	Description of Change	Prepared – Reviewed – Approved
		enrolled in the group health, life and accident insurance policy, who give their own explicit consent on the family-member attachment to form PIMS-FM-001-B	



Table of Contents

Purpose.....	6
1. Privacy Notice	6
1.1 Who we are.....	6
1.2 What we collect, why, and on what lawful basis	6
1.3 Who we share it with	10
1.4 Transfers outside Thailand.....	10
1.5 How long we keep it	11
1.6 Your rights	12
Document Approval	13



Purpose

This notice explains how DailiTech collects, uses, discloses and protects your personal data, and the rights you have under the Personal Data Protection Act B.E. 2562 (2019).

1. Privacy Notice

1.1 Who we are

DailiTech Co., Ltd. ("DailiTech", "we") is the data controller. This notice applies to DailiTech employees, personnel (including interns, trainees and contract staff) and, where relevant, former employees. It also applies to family members enrolled in the group health, life and accident insurance policy. You can contact our Data Protection Officer at privacy@dailitech.com, telephone 02-105-3296, or The Parq, 6th Floor Unit, East Wing, 88 Ratchadaphisek Road, Klongtoey, Bangkok 10110, Thailand.

1.2 What we collect, why, and on what lawful basis

Activity	Personal data	Purpose	Lawful basis
Identity & Access Management	Name, email address	SSO/MFA authentication for all tools, Conditional Access, onboarding/offboarding provisioning	Contract (PDPA s.24(3))
Device Management (Microsoft Intune MDM)	Employee name (device-to-user association)	Manage devices: configuration profiles, patch management, FileVault, USB policy, remote wipe	Legitimate interest (PDPA s.24(5))
Microsoft Teams Meeting Recording (internal and customer meetings)	Participant full names, image and voice	Record Teams meetings for review, work handover and as audit evidence	Legitimate interest (PDPA s.24(5))
AWS Access Provisioning and Revocation	Employee name	Control engineers' IAM role access to customer AWS accounts	Contract (PDPA s.24(3))
Corporate Email Communication (Microsoft 365 Exchange + Purview)	Name, email address	Send and receive business email with customers, suppliers and partners under DLP and sensitivity-label controls	Contract (PDPA s.24(3))
Personal Income Tax Withholding and Remittance	Full name, national ID number, taxpayer ID, income, allowances, tax withheld	Calculate and remit employees' personal income tax withheld at source to the Revenue Department	Legal obligation (PDPA s.24(6))



Activity	Personal data	Purpose	Lawful basis
Social Security Contributions and Benefits	Full name, national ID number, social security number, wages, sickness/maternity information (when claiming benefits)	Remit social security contributions and administer employees' social security benefits	Legal obligation (PDPA s.24(6)); PDPA s.26(5)(c) for health data required under social security law
Group Health Insurance Administration	Full name, national ID number, date of birth, claim history, diagnosis / medical certificate; annual health check results (e.g. weight, height, blood pressure, blood group, medical history, disability); details and health data of insured family members	Administer employees' group health insurance (enrolment, claims, policy renewal); annual health checks; life and accident insurance for employees and their family members; insurance claims, amendments and cancellations	Contract (PDPA s.24(3)); explicit consent (PDPA s.26) for health data, given on form PIMS-FM-001-B (Section 1) by the employee and on its family-member attachment by each insured family member (a parent or guardian for a minor)
Personnel Administration and Performance Appraisal	Full name, nickname, date of birth, age, gender, nationality, photograph, national ID number, address, telephone number, personal email, emergency contact (name, relationship, telephone number), education history and qualifications, job application form, CV/resume and work history, interview and test results, professional licences, employee ID, employment contract, leave records, time attendance and overtime records, appraisal results, training history, warning letters, transfers and promotions, resignation or termination documents and reasons, military service status, driving licence number, vehicle registration number	Maintain personnel files, employment contracts, leave, appraisals and staff development; time attendance, overtime and holiday work; appointments, transfers and changes of position; employment certificates; work assignments and authorisations; awards and scholarships; training, seminars, study visits and meetings inside and outside the company (travel arrangements are covered under Business Travel); keeping former employees' records for business continuity and possible legal disputes	Contract (PDPA s.24(3)); legitimate interest (PDPA s.24(5)) for former employees' records and work-related events



Activity	Personal data	Purpose	Lawful basis
Post-hire Criminal Record Check (all positions)	Criminal record certificate issued by the Royal Thai Police and provided by the employee (full name, national ID number, result); outcome of HR's review	Assess suitability for the employee's role. HR reviews the certificate; where a record is disclosed, HR and the Managing Director assess it case by case against the requirements of the role.	Explicit consent (PDPA s.26), given on form PIMS-FM-001-B (Section 2)
Payroll, Compensation and Welfare Benefits	Full name, employee ID, salary and other compensation, bank account number and bank details, provident fund membership, welfare claims (medical expenses not covered by group health insurance, education allowance for family members, housing and utilities), marital status, family members' details and supporting documents	Pay salaries and compensation, including salary adjustments; administer the provident fund and welfare benefits	Contract (PDPA s.24(3))
Work Permit and Visa (foreign employees)	Full name, nationality, passport number, visa, work permit, photograph, education certificates, employment history, criminal record (where required by the authority)	Apply for, renew and maintain work permits and visas with the Department of Employment and the Immigration Bureau, through legal advisers where engaged	Legal obligation (PDPA s.24(6)); explicit consent (PDPA s.26) for criminal record
Business Travel (domestic and overseas)	Full name (as in passport), date of birth, nationality, passport number and copy of passport, passport expiry date, visa, telephone number, email, flight and accommodation details, travel insurance details, emergency contact (name, relationship, telephone number)	Arrange business trips, customer visits, training and events in Thailand and abroad: visa applications, flight and hotel bookings, travel insurance, and contacting your emergency contact in case of an emergency during travel	Contract (PDPA s.24(3)); vital interest (PDPA s.24(2)) for contacting the emergency contact in an emergency
Submission of Personnel Profiles to Customers	Full name, position, profile/CV (work history and project experience), education history, professional certifications and training	Present the project team in proposals, tenders (TOR/e-bidding) and project staffing plans, and meet customer requirements on team qualifications	Legitimate interest (PDPA s.24(5)); contract (PDPA s.24(3)) where required to perform the customer contract



Activity	Personal data	Purpose	Lawful basis
Use of Employee Photographs and Videos in Social Media, Advertising and Marketing	Full name, position, photographs, video and voice, quotes or testimonials	Publish on the company website and social media (e.g. LinkedIn, Facebook), and use in advertising, marketing and recruitment materials, events and company news	Consent (PDPA s.19), which you may refuse or withdraw at any time without affecting your employment; legitimate interest (PDPA s.24(5)) for incidental appearance in event or group photographs, with the right to object
Monitoring of IT Resources and Electronic Communications	Records generated by Identity & Access Management, Device Management and Corporate Email (sign-in logs, device information, email and DLP events), endpoint security events (CrowdStrike Falcon), IP address, browser information and cookies	Ensure company IT resources, accounts and devices are used properly and securely in accordance with company policy and the law; investigate security incidents	Legitimate interest (PDPA s.24(5)); legal obligation (PDPA s.24(6))
Office CCTV	Video images	Record video in office areas for the safety of persons and property	Legitimate interest (PDPA s.24(5))

Sensitive personal data: Social Security Contributions and Benefits – health data (benefit claims); Group Health Insurance Administration – health data (including annual health check results, blood group and disability) of employees and insured family members; Post-hire Criminal Record Check – criminal record (all employees); Work Permit and Visa – criminal record. We process sensitive data only with your explicit consent or where permitted by PDPA Section 26.

Sources of personal data: We collect personal data directly from you (e.g. job application, employment contract, CV/resume, identity documents, interviews, requests and communications with us) and from other sources such as recruitment agencies, job websites, referees, government agencies and service providers that collect data on our behalf.

Personal data of other persons: If you provide personal data of other persons to us (e.g. family members or emergency contacts), please inform them of this notice before providing their data, so that we can obtain their consent where required. Family members enrolled in the group health, life and accident insurance policy give their own consent on the family-member attachment to form PIMS-FM-001-B when they are enrolled.



New purposes: If we need to use your personal data for a purpose not described in this notice, we will inform you of the new purpose and obtain your consent where required.

1.3 Who we share it with

- IT and cloud service providers: Microsoft Corporation (Microsoft 365), tldv GmbH, Notion Labs, Make (Celonis SE), Amazon Web Services (AWS), Airtable
- Payroll and accounting service providers: outsourced accounting firm (bookkeeping, payroll, personal income tax withholding and social security filings)
- Banks and financial institutions: salary payment; provident fund manager
- Insurance and healthcare providers: partner insurance company, partner hospitals
- Government agencies: Revenue Department, Social Security Office, Department of Employment, Immigration Bureau (foreign employees)
- Legal advisers and professional service providers: e.g. work permit and visa applications
- Customers and prospective customers (including government agencies): profiles/CVs and education history submitted in proposals, tenders and project staffing
- Social media platforms and the public: photographs and videos published with your consent on the company website and social media
- Travel and event service providers: airlines, hotels, travel agencies, travel insurers, catering and venue providers, embassies and consulates, and customers or event hosts at the destination (business travel, training, seminars and work-related events)
- Building management and CCTV service provider: The Parq
- DailiTech affiliated companies: only personnel who need the data for the purposes above
- Law enforcement agencies, regulators and courts: where required by law or court order
- Prospective acquirers or successors: in a restructuring, merger or sale of business

1.4 Transfers outside Thailand

Some of our service providers store or process data outside Thailand. We transfer data only where the destination country has adequate data protection standards, where appropriate safeguards are in place (such as the provider's data processing terms incorporating standard contractual clauses), or where an exception under PDPA Section 28 applies:

- Microsoft Corporation – Microsoft global cloud (data residency: Southeast Asia)



- tldv GmbH – Germany (European Union)
- Notion Labs, Inc. – United States
- Make (Celonis SE) – European Union (Czech Republic)
- Amazon Web Services, Inc. – Singapore (ap-southeast-1), Thailand (ap-southeast-7), United States (us-east-1)
- Airtable, Inc. – United States
- Business travel abroad – airlines, hotels, travel agencies, embassies/consulates and hosts in the destination country, only as necessary to arrange the trip (PDPA Section 28(3) – necessary for the performance of the employment contract)
- Social media platforms (e.g. LinkedIn, Facebook) – content published with your consent may be stored outside Thailand and accessed worldwide (PDPA Section 28 – consent)

1.5 How long we keep it

- Identity & Access Management: Employment duration + 3 years after termination (audit logs)
- Device Management (Microsoft Intune MDM): Duration of employment
- Microsoft Teams Meeting Recording (internal and customer meetings): Up to 5 years (internal meetings) / as specified in the DPA (customer meetings)
- AWS Access Provisioning and Revocation: 2 years (access logs) / project duration (active assignments)
- Corporate Email Communication (Microsoft 365 Exchange + Purview): Up to 10 years (emails constituting contractual evidence – highest label) / 1–5 years by sensitivity label
- Personal Income Tax Withholding and Remittance: At least 5 years and not more than 10 years, in accordance with the Revenue Code
- Social Security Contributions and Benefits: Employment duration + at least 2 years and not more than 10 years
- Group Health Insurance Administration: Policy period + 2 years after the end of the policy or employment
- Personnel Administration and Performance Appraisal: Employment duration + 5 years; employment contracts and termination documents up to 10 years (limitation period)



- Post-hire Criminal Record Check: certificate and the outcome of HR's review are kept in the HR employee file, with access limited to HR (and the Managing Director where a record is disclosed), for the personnel-file retention period
- Office CCTV: 30 days
- Payroll, Compensation and Welfare Benefits: 10 years after termination of employment
- Work Permit and Visa (foreign employees): 10 years after termination of employment
- Business Travel (domestic and overseas): 10 years after termination of employment
- Submission of Personnel Profiles to Customers: Up to 3 years (proposal not awarded) / contract duration + 10 years (awarded)
- Use of Employee Photographs and Videos in Social Media, Advertising and Marketing: Until consent is withdrawn; content is then removed from channels controlled by DailiTech (printed materials already distributed cannot be recalled)
- Monitoring of IT Resources and Electronic Communications: As for the source activity (Identity & Access Management, Device Management, Corporate Email); investigation records until the matter is closed plus the applicable limitation period

Where a longer retention period is required or permitted by law, or is needed for the establishment, exercise or defence of legal claims, we may retain the data for that longer period.

1.6 Your rights

You have the right to be informed of how we collect, use and disclose your data, to access and obtain a copy of your data, data portability, objection, erasure, restriction and rectification, to withdraw consent where processing is based on consent (withdrawal does not affect processing carried out before the withdrawal), and to lodge a complaint with the Personal Data Protection Committee. To exercise your rights, contact privacy@dailitech.com, telephone 02-105-3296, or use form PIMS-FM-002. If you do not provide personal data needed for a contract or legal obligation, we may be unable to enter into or perform the contract or comply with the law.



Document Approval

Prepared by	Reviewed by	Approved by
Signature (Sura Rodpongpun) PIMS Working Team and DPO Date 19 / 10 / 2026	Signature (Vit Niennattrakul) Managing Director Date 19 / 10 / 2026	Signature (Vit Niennattrakul) Managing Director Date 19 / 10 / 2026