

Combo Technology Privacy Policy

Last Updated: 22 October 2026 (Version 1.1)

1. Introduction

This Policy explains how COMBO TECHNOLOGY PTE. LTD. (the Company) handles personal data under Singapore's Personal Data Protection Act 2012 (PDPA). It covers website users, customers, business contacts, job applicants, employees and former employees. The Employee Personal Data section provides the notice relevant to employment.

2. Data Collection

We collect relevant identity and contact information, communications, service or transaction records, and website or system usage information. Employment data categories and sources are described below. We limit collection to what is reasonably needed for a notified purpose or permitted by law; national identifiers are collected only where legally required or otherwise permitted.

3. Purpose of Data Use

We use relevant data to respond to enquiries, deliver and administer services, maintain accounts, improve service reliability, protect systems, investigate misuse, and comply with legal duties. We explain new purposes before processing where required. Marketing or unrelated publicity requires an appropriate lawful basis and separate consent where required; employment acknowledgement does not authorise marketing.

4. Data Sharing

We do not sell or rent personal data. Where necessary for the relevant purpose, we share it with authorised personnel, contracted service providers, professional advisers, and authorities as required or permitted by law. Related COMBO entities receive it only for a specific necessary purpose and with appropriate safeguards. Approval, confidentiality and security requirements apply; a group relationship alone does not authorise access.

5. Data Security

We use reasonable safeguards appropriate to sensitivity and risk, including access restrictions, approved systems, secure transfer and disposal, and encryption where appropriate or required by Company policy. Access is limited to authorised persons with a work need. Suspected personal-data incidents must be reported immediately to IT, HR or the data protection contact so that assessment and any required notifications can be coordinated.

6. Your Rights

Subject to applicable legal exceptions, you may request access to your personal data and information about its use or disclosure in the preceding year, or request correction of an error or omission. We verify identity before releasing data and explain any applicable refusal, fee or further time needed.

You may withdraw consent for consent-based processing by writing to the contact below. We explain likely consequences and stop the relevant processing within a reasonable period as required by law. Withdrawal does not prevent processing that remains required or authorised by law, or require deletion of records that must lawfully be retained.

7. Retention and Overseas Transfers

We review retention needs and securely delete or anonymise data when its purpose is no longer served and retention is no longer needed for legal or business purposes. The approved retention schedule and any lawful evidence hold apply. ISP20 requires disposal of employee PII no longer in use within five years, and customer PII within one month, subject to legal requirements and documented holds. These are outer disposal limits, not reasons to retain unnecessary data for the full period.

Approved cloud, HR or shared-service arrangements may involve storage or access outside Singapore. Before such transfers, the Company must establish safeguards providing protection comparable to the PDPA, unless a lawful exception applies. Provider, destination, access and contractual safeguards must be reviewed; signing this Policy or an acknowledgement does not waive these requirements.

8. Employee Personal Data

Scope and categories. For applicants, current staff and former staff of the Company, relevant data may include identity and work-eligibility records; contact and emergency-contact details; CVs, qualifications, employment and reference checks; bank, salary, CPF, tax and benefit records; leave and necessary health or insurance information; performance, training and disciplinary records; asset, account, access and security records. Sensitive records are restricted to persons who need them.

Employment purposes. We process relevant data for recruitment and screening; entering into, managing or ending employment; payroll, statutory contributions, tax and work-pass administration; benefits, leave, training and performance; workplace safety and security; asset and access management; investigations, audits, disputes, and compliance. Checks must be lawful and proportionate to the role. Credit checks or other intrusive checks are not authorised merely by this notice.

Sources and other people's details. Data may come from you, authorised recruiters, references, relevant public sources, authorities and service providers where lawful. Before providing an emergency contact's or dependant's data, inform that person of the relevant purpose and obtain permission where required. The Company must separately satisfy its own legal obligations.

Recipients. Necessary employment data may be shared with authorised HR, managers, Board members and IT personnel; approved payroll, HR, benefits, insurance, medical, banking, Lark and cloud-service providers; advisers or auditors; and CPF Board, IRAS, MOM or other relevant authorities. Customers or partners receive only necessary work contact or role information, or other data supported by a specific lawful purpose. Overseas sharing remains subject to the safeguards above.

Notice and consent. Where reasonable for entering into, managing or terminating employment, or another PDPA exception applies, consent may not be required. The Company must still provide employment-purpose notification as required. For a new unrelated use, we notify you and obtain specific consent where required. Optional event-image publicity is recorded separately, is not a condition of employment or benefits, and is not authorised by a general acknowledgement. Declining it does not prevent routine lawful employment processing.

Workplace systems. Where implemented and notified, office CCTV, access logs and Company-system or device records may be used proportionately for safety, security, asset control, service operations and investigations. This does not authorise unrestricted access to private accounts or personal-device content. Additional monitoring or collection requires an appropriate notice and lawful basis.

Staff responsibilities. Handle employee, customer and partner personal data only for approved duties, use approved storage and transfer channels, apply classification and access rules, and never put it into unapproved personal, cloud or AI tools. Follow ISP20 and related security policies, complete assigned training, and report suspected loss or disclosure immediately. Confidentiality and lawful retention duties continue after departure.

Acknowledgement and changes. HR provides the current Policy and relevant briefing and retains a dated acknowledgement. Optional consents are recorded separately. Staff should keep their information accurate and may use the request channel above. Material changes are communicated before a new use where required. Existing staff sign on the actual receipt/signing date; an acknowledgement does not retrospectively authorise earlier processing.

9. Updates to This Policy

We may revise this Policy and update its version and date. We communicate material changes through appropriate channels, including HR or Lark for employees. A new consent-based purpose requires fresh consent where applicable; publication of an update alone does not create that consent.

10. Contact Us

For privacy questions, access or correction requests, withdrawal of consent, complaints or personal-data incident reports, contact hr@51combo.com, marked for the attention of the Data Protection Officer. The Company will maintain an appointed DPO and a current, accessible contact channel.

COMBO TECHNOLOGY PTE. LTD.
6 Shenton Way, #24-08, OUE Downtown 2
Singapore 068809