Data Protection & Privacy Policy

FC-DPO-P-001

Ver 1.0

Forecepts Pte Ltd (Reg. No. 201133876C)

14 Arumugam Road Building C, #05-07 Singapore 409959

info@forecepts.com

Document Control

Document Owner	Data Protection Officer
Document Classification	Internal Use
Applicable Standard	ISO/IEC 27001:2022 Annex A.5.34; Singapore PDPA 2012 (as amended 2020); Malaysia PDPA 2010 (Act 709, as amended by Act A1727); Indonesia UU PDP 2022 (Law No. 27/2022)
Review Frequency	At least annually, or as and when needed (e.g. a material change to the SaaS platform, processing activities, applicable data protection legislation in Singapore, Malaysia or Indonesia, or organisational structure)
Retention	This Policy and related records shall be retained in accordance with FC-DPO-P-002 Data Retention & Disposal Policy

Change History

Date	Version	Prepared By	Remarks	Approved By
1 JAN 2026	1.0		Initial issue	

Table of Contents

1 Purpose

This Policy sets out how Forecepts Pte Ltd ("Company") collects, uses, discloses, stores, protects and disposes of personal data in compliance with the data protection laws of all three jurisdictions in which it operates: Singapore's Personal Data Protection Act 2012 (PDPA); Malaysia's Personal Data Protection Act 2010 (Act 709, as amended); and Indonesia's Law No. 27/2022 on Personal Data Protection (UU PDP).

This Policy applies alongside the Company's ISMS policies and the supporting SOPs, forms and registers listed in Section 7.

2 Scope

This Policy applies to all personal data processed by the Company, whether as:

- data controller (for the personal data of its employees, vendors, corporate client administrators and, where applicable, direct customer data); or
- data intermediary/processor (for traveller and customer personal data processed on behalf of client under written SaaS agreements).

It covers all employees, contractors and systems across the Company's Singapore, Malaysia and Indonesia operations, including data hosted on AWS Singapore. Where the Company acts as data intermediary/processor, this Policy addresses the Company's own obligations; it does not replace the client's own obligation as controller to comply with applicable data protection law.

3 References

- FC-DPO-REG-01 Legal Compliance Register – SG PDPA 2012 (Act)
- FC-DPO-REG-01a Legal Compliance Register – SG Personal Data Protection Regulations 2021
- FC-DPO-REG-04 Legal & Other Requirements Register – Malaysia PDPA 2010 + PDP Regulations 2013
- FC-DPO-REG-07 Legal & Other Requirements Register – Indonesia UU PDP 2022
- FC-DPO-P-002 Data Retention & Disposal Policy
- FC-DPO-SOP-001 Personal Data Breach Notification Procedure
- FC-DPO-SOP-002 Data Subject Access Request (DSAR) Procedure
- FC-DPO-SOP-003 Privacy Impact Assessment (DPIA/PIA) Procedure
- FC-DPO-SOP-004 Data Transfer & Cross-Border Transfer Procedure
- FC-ISMS-P-009 Data Classification & Handling Policy
- FC-ISMS-P-010 BYOD Policy
- FC-IT-P-001 IT Usage & Security Policy
- Statement of Applicability (SoA)

4 Terms and Definitions

Term / Abbreviation	Definition
Personal Data	Data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access, whether or not in electronic form (SG PDPA s.2; MY PDPA s.4; ID UU PDP Art.1).
Sensitive / Specific Personal Data	Categories of personal data subject to heightened protection under applicable law, including health data, biometric data, financial account information, children's data, criminal records, political opinions and religious beliefs (MY PDPA s.40; ID UU PDP Art.4).
Data Subject	An identified or identifiable individual to whom personal data relates.
Data Controller / Organisation	An entity that determines the purposes and means of processing personal data ("organisation" under SG PDPA; "data user/data controller" under MY PDPA; "Pengendali Data Pribadi" under ID UU PDP).
Data Intermediary / Processor	An entity that processes personal data on behalf of, and for the purposes of, a controller, under a contract evidenced in writing ("data intermediary" under SG PDPA; "data processor" under MY PDPA and ID UU PDP).
Consent	Voluntary, informed indication of agreement by the data subject to the processing of their personal data for one or more specified purposes.
Personal Data Breach	Unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data, or loss of a storage medium or device on which personal data is stored, or a failure of protection of the confidentiality, integrity or availability of personal data, however caused.
DPO	Data Protection Officer — the individual designated under SG PDPA s.11(3), MY PDPA s.12A, and in practice for Indonesia operations.
PDPC	Singapore's Personal Data Protection Commission.
JPDP	Jabatan Perlindungan Data Peribadi — Malaysia's Personal Data Protection Department.
Komdigi / MOCD	Indonesia's Ministry of Communication and Digital, exercising PDP oversight functions pending establishment of the independent PDP Agency (Lembaga PDP) under UU PDP Art.58.

5 Roles and Responsibilities

5.1 Top Management shall:

- Approve and endorse this Policy and allocate the resources necessary for its implementation;
- Ensure that the Company's data protection obligations are met across all three jurisdictions;
- Approve external regulatory notifications and engagement of external counsel where required.

5.2 The DPO shall:

- Ensure it remains current against applicable law in Singapore, Malaysia and Indonesia;
- Advise the Company on its data protection obligations and monitor compliance;
- Maintain the DPO document suite (policies, SOPs, forms, registers) and the DPIA/PIA Register;

- Act as the primary point of contact for the PDPC, JPDP, Komdigi/MOCD and for data subjects exercising their rights;
- Report to Top Management on the Company's data protection posture.

5.3 IT Department

IT shall:

- Implement and maintain the technical controls necessary to protect personal data (encryption, access controls, logging, backup);
- Support the DPO in investigating and containing data breaches;
- Suspend or resume automated deletion or disposal jobs on the DPO's instruction.

5.4 Project Team

The Project Team shall:

- Screen new projects, features, vendors and sub-processors for data protection impact per FC-DPO-SOP-003 Privacy Impact Assessment (DPIA/PIA) Procedure;
- Coordinate with corporate clients on any change materially affecting traveller or customer data;
- Support the DPO in identifying which client(s) and jurisdiction(s) are affected by a breach or a data subject request.

5.5 HR/Admin

HR/Admin shall act as first point of contact for data protection matters relating to employees and former employees, and forward such matters to the DPO.

5.6 All Employees and Contractors

- Handle personal data only for authorised business purposes and in accordance with this Policy;
- Report any suspected or actual personal data breach to the DPO and IT immediately, and in any event within 24 hours;
- Not attempt to independently investigate, alter or conceal a suspected breach;
- Complete data protection awareness training.

6 Policy Statements

The following statements set out the Company's data protection commitments. Each statement is grounded in the applicable legal requirements documented in the Company's legal registers (FC-DPO-REG-01, 01a, 04, 07) and is supported by the SOPs, forms and registers listed in 3.Reference.

6.1 Accountability and Governance

The Company shall designate a Data Protection Officer to be responsible for ensuring compliance with this Policy and applicable data protection law. The DPO's business contact information shall be published on the Company's website and registered with ACRA (Singapore) and made available for Malaysia and Indonesia operations.

The Company shall develop and implement the policies, procedures and practices necessary to meet its obligations, and shall make information about these policies and practices available on request (SG PDPA s.12; MY PDPA s.5; ID UU PDP Art.35–39).

6.2 Consent and Legal Basis for Processing

The Company shall only collect, use or disclose personal data where:

- the individual has given valid consent; or
- the processing is permitted under another lawful basis recognised by the applicable data protection law.

Consent must be given freely, be based on clear information and relate to a specific purpose.

Where the Company relies on deemed consent under the Singapore PDPA, the DPO shall document the applicable basis.

Where consent is not required, the Company shall identify and record the applicable lawful basis before processing begins. This may include processing that is necessary to:

- perform a contract;
- comply with a legal obligation;
- protect the vital interests of an individual; or
- meet another lawful purpose permitted by the applicable law.

The applicable requirements include Sections 13 to 17 and the First and Second Schedules of the Singapore PDPA, Section 6 of the Malaysian PDPA, and Articles 20 to 24 of Indonesia's Personal Data Protection Law.

6.3 Notice and Transparency

The Company shall provide individuals with a privacy notice on or before collecting their personal data. The notice shall clearly explain:

- why the personal data is being collected, used or disclosed;
- the types of third parties to whom the data may be disclosed; and
- how the individual may contact the DPO regarding their personal data.
    - a description of the personal data being collected;
    - the source of the personal data, where it was not collected directly from the individual;
    - the individual's right to access and correct their personal data, and how to exercise it;
    - the choices and means available to the individual to limit the processing of their personal data; and
    - whether the supply of the personal data is obligatory or voluntary, and the consequences of not supplying it.

Privacy notices shall be written in clear, simple and accessible language.

Where the Company processes personal data as a data intermediary or processor on behalf of a client, the client is responsible for providing the privacy notice to its own data subjects. The Company shall provide reasonable support to the client in meeting this obligation, as required under the applicable SaaS agreement.

This requirement supports compliance with Section 20 of the Singapore PDPA, Section 7 of the Malaysian PDPA and Article 5 of Indonesia's Personal Data Protection Law.

6.4 Purpose Limitation

The Company shall collect, use and disclose personal data only for legitimate and appropriate purposes that have been communicated to the individual or for which valid consent has been obtained.

Personal data shall not be used for a new or unrelated purpose unless:

- the individual has been informed and, where required, has provided fresh consent; or
- another lawful basis applies and has been documented.

This requirement supports compliance with Section 18 of the Singapore PDPA, Section 5 of the Malaysian PDPA and Article 16 of Indonesia's Personal Data Protection Law.

6.5 Accuracy

The Company shall take reasonable steps to ensure that personal data is accurate, complete and up to date.

Particular care shall be taken where the personal data:

- is used to make a decision that may affect an individual; or
- is disclosed to another organisation.

This requirement supports compliance with Section 23 of the Singapore PDPA, Section 11 of the Malaysian PDPA and Articles 27 to 29 of Indonesia's Personal Data Protection Law.

6.6 Protection and Security

The Company shall implement reasonable and appropriate security measures to protect personal data in its possession or under its control against unauthorised access, collection, use, disclosure, copying, alteration, loss, disposal or other similar risks.

Security measures shall be proportionate to the nature, sensitivity and risk of the personal data and may include:

- technical measures, such as encryption at rest and in transit, access controls, multi-factor authentication and security logging;
- organisational measures, such as policies, employee training, confidentiality obligations and access reviews; and
- physical measures, where applicable, such as secure work areas and controlled access to equipment or records.

All employees using personal devices for Company work shall comply with FC-ISMS-P-010 BYOD Policy, including the requirements for VPN use, multi-factor authentication and automatic screen lock.

Further security requirements are set out in FC-IT-P-001 IT Usage & Security Policy and the Company's Statement of Applicability.

This requirement supports compliance with Section 24 of the Singapore PDPA, Section 9 of the Malaysian PDPA and Articles 35 to 39 of Indonesia's Personal Data Protection Law.

6.7 Retention and Disposal

The Company shall retain personal data only for as long as necessary to:

- fulfil the purpose for which it was collected;
- meet legal, regulatory or contractual requirements; or
- support a legitimate business need.

When personal data is no longer required, the Company shall securely delete, destroy or anonymise it so that it can no longer be linked to an individual.

Retention periods and approved disposal methods are specified in FC-DPO-P-002 Data Retention & Disposal Policy.

This requirement supports compliance with Section 25 of the Singapore PDPA, Section 10 of the Malaysian PDPA and Articles 43 to 45 of Indonesia's Personal Data Protection Law.

6.8 Access and Correction

Individuals may request access to, or correction of, their personal data held by the Company.

The Company shall process each request in accordance with the applicable legal timeframe:

- Singapore: As soon as reasonably possible. Where the Company cannot respond within 30 days, it shall inform the individual in writing of the expected response time.
- Malaysia: Within 21 days, subject to any extension permitted by law.
- Indonesia: Correction requests shall be completed within three days (3 × 24 hours), and access requests shall be handled as soon as reasonably possible.

Detailed requirements for receiving, verifying and responding to requests are set out in FC-DPO-SOP-002 Data Subject Access Request (DSAR) Procedure.

This requirement supports compliance with Sections 21 to 22A of the Singapore PDPA, Sections 30 to 37 of the Malaysian PDPA and Articles 6, 8 and 30 to 33 of Indonesia's Personal Data Protection Law.

6.9 Consent Withdrawal

An individual may withdraw consent to the collection, use or disclosure of personal data by providing reasonable notice.

Upon receiving a valid withdrawal request, the Company shall:

- inform the individual of the likely consequences of withdrawing consent;

- stop the relevant processing, unless continued processing is permitted or required by law; and
- notify relevant service providers or other parties where necessary.

For requests governed by Indonesian law, the Company shall stop the relevant processing within three days (3 × 24 hours) of receiving a valid withdrawal.

This requirement supports compliance with Section 16 of the Singapore PDPA, Section 38 of the Malaysian PDPA and Articles 40 to 42 of Indonesia's Personal Data Protection Law.

6.10 Cross-Border Transfer

The Company shall only transfer personal data outside the jurisdiction in which it was collected where appropriate safeguards are in place.

Before a transfer takes place, the Company shall ensure that:

- the recipient provides a standard of protection comparable to that required by applicable law;
- an appropriate contractual, regulatory or other lawful transfer mechanism is in place; or
- another permitted exception applies.

Cross-border transfers shall be assessed in accordance with FC-DPO-SOP-004 Data Transfer & Cross-Border Transfer Procedure and, where required, documented through a Transfer Impact Assessment.

This requirement supports compliance with Section 26 of the Singapore PDPA, Section 129 of the Malaysian PDPA and Articles 55 to 56 of Indonesia's Personal Data Protection Law.

6.11 Data Breach Notification

The Company shall promptly identify, assess, contain and manage any personal data breach in accordance with FC-DPO-SOP-001 Personal Data Breach Notification Procedure.

Where required by applicable law, the Company shall notify the relevant regulator and affected individuals within the following timelines:

- Singapore: Notify the PDPC as soon as practicable and no later than three calendar days after determining that the breach is notifiable. Affected individuals shall be notified as soon as practicable, where required.
- Malaysia: Notify the Personal Data Protection Commissioner as soon as practicable and no later than 72 hours. Where the breach is likely to cause significant harm, affected individuals shall be notified without unnecessary delay and no later than seven days after the initial notification to the Commissioner.
- Indonesia: Provide written notification to affected individuals and the relevant authority within three days (3 × 24 hours) of the breach.

Where the Company processes personal data on behalf of a client, it shall notify the client without undue delay and support the client in meeting its breach-notification obligations.

These requirements support compliance with Sections 26A to 26E of the Singapore PDPA, Section 12B of the Malaysian PDPA and Article 46 of Indonesia's Personal Data Protection Law.

6.12 Data Protection Impact Assessment

The Company shall conduct a DPIA/PIA before introducing any new or significantly changed personal data processing activity that is likely to create a high privacy risk.

The assessment shall be conducted in accordance with FC-DPO-F-003 Project Risk Assessment Form.

A DPIA is required for high-risk processing under Article 34 of Indonesia's Personal Data Protection Law. The Company also applies DPIA/PIA assessments as a standard risk-management and accountability practice for its Singapore and Malaysian operations.

6.13 Sensitive and Specific Personal Data

The Company shall only process sensitive or specific personal data where there is a valid legal basis, including explicit consent where required, or where the processing is permitted or required by law.

Additional security and access controls shall be applied according to the sensitivity and risk of the data. These controls are specified in FC-ISMS-P-009 Data Classification & Handling Policy.

This requirement supports compliance with Section 40 of the Malaysian PDPA and Article 4 of Indonesia's Personal Data Protection Law.

6.14 Direct Marketing

The Company shall only use personal data for direct marketing where permitted by applicable law and, where required, with the individual's consent.

The Company shall:

- comply with Singapore's Do Not Call Registry requirements for marketing messages sent to Singapore telephone numbers;
- comply with applicable Malaysian direct-marketing objection and opt-out requirements; and
- include a clear and working unsubscribe or opt-out method in all marketing communications.

The Company shall stop sending marketing communications within a reasonable period after receiving a valid opt-out request.

This requirement supports compliance with Part 9 of the Singapore PDPA and Section 43 of the Malaysian PDPA.

6.15 Children's Data and Vulnerable Individuals

The Company shall apply additional safeguards when processing personal data relating to children or vulnerable individuals.

The Company shall not knowingly collect or process a child's personal data without verifiable consent from a parent or lawful guardian where such consent is required.

For processing governed by Indonesian law, the Company shall comply with the specific requirements relating to children including the involvement of a parent, guardian or authorised representative where legally required.

This requirement supports compliance with Articles 25 and 26 of Indonesia's Personal Data Protection Law.

6.16 Data Portability

Individuals whose personal data is governed by Malaysian law may request that their personal data be transferred directly to another data controller, subject to technical feasibility, compatible data formats and any other applicable legal requirements.

Where the Company acts as the data controller, it shall assess and respond to the request in accordance with applicable law.

Where the Company acts as a data processor on behalf of a client, it shall provide reasonable assistance to the client in handling the request, as required under the applicable SaaS agreement.

This requirement supports compliance with Section 43A of the Malaysian PDPA.

6.17 Unauthorised Re-Identification of Anonymised Information

The Company shall not knowingly or recklessly re-identify, or attempt to re-identify, an individual from anonymised information, except where a statutory defence or exception applies.

Re-identification for a legitimate purpose, such as testing the Company's own anonymisation methods, shall be authorised in advance by the DPO, and any re-identified data shall be immediately re-secured or destroyed once that purpose is fulfilled.

Any suspected or actual unauthorised re-identification shall be reported to the DPO immediately in accordance with FC-DPO-SOP-001 Personal Data Breach Notification Procedure.

This requirement supports compliance with Section 48F of the Singapore PDPA.

6.18 Third-Party Disclosure and Vendor Controls

The Company shall not disclose personal data to any third party except where:

- the individual has given valid consent to the disclosure;
- the disclosure is permitted or required under applicable data protection law or another legal obligation; or
- the disclosure is made to a vendor, sub-processor or service provider under a binding written agreement that requires the recipient to protect the personal data to a standard comparable to that required by applicable law.

Before engaging any vendor or sub-processor that will process personal data on the Company's behalf, the DPO or a designated representative shall conduct a data protection assessment to confirm that adequate safeguards are in place. Approved vendors and sub-processors shall be recorded in the Company's Third-Party / Sub-Processor Register.

Vendors and sub-processors shall be permitted to process personal data only for the specific purposes set out in the applicable agreement, and shall not further disclose or sub-contract the processing of personal data without the Company's prior written authorisation.

Where a vendor or sub-processor suffers a personal data breach affecting the Company's data, the Company shall be notified without undue delay, and the incident shall be managed in accordance with FC-DPO-SOP-001 Personal Data Breach Notification Procedure.

This requirement supports compliance with Section 4(1A) of the Singapore PDPA, Section 44 of the Malaysian PDPA and Articles 53 to 54 of Indonesia's Personal Data Protection Law.

6.19 Public Availability of Privacy Information

The Company is committed to being open and transparent about how it handles personal data.

This Policy, or a plain-language summary of it, shall be published on the Company's website and kept current. Individuals shall be able to access it at any time without the need to make a formal request.

The publication shall include, at minimum:

- the types of personal data the Company collects and the purposes for which it is processed;
- how individuals may exercise their rights, including access, correction, withdrawal of consent and erasure; and
- the name, role and business contact details of the DPO.

Any material update to this Policy shall be reflected on the website within 14 days of the effective date of the change.

Where the Company processes personal data as a data intermediary on behalf of a client, the client remains responsible for publishing its own privacy notice to its data subjects. The Company shall provide reasonable support to the client in meeting this obligation, as required under the applicable SaaS agreement.

This requirement supports compliance with Section 12 of the Singapore PDPA, Section 5 of the Malaysian PDPA and Article 35 of Indonesia's Personal Data Protection Law.

7 Related Documents

Document Number	Record / Form / Procedure
FC-DPO-F-002	Data Subject Access & Correction Request Log
FC-DPO-F-006	Law Enforcement Request Log
FC-DPO-F-003	Project Risk Assessment Form
FC-ISMS-F-005	Corrective Action Report
FC-ISMS-F-018	BYOD Device Registration Form
FC-ISMS-F-024	Clear Desk & Clear Screen Compliance Checklist
FC-IT-F-004	Information Security Incident Report Form