DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is made as of the date of the Client's signature below.

BETWEEN:

1. The "**Client**" as identified on the signature page of this DPA or as otherwise identified in an executed Agreement that explicitly incorporates this DPA; and

2. Frankie Financial Pty Ltd (ABN 61 623 506 892) of Level 6, 440 Collins Street, Melbourne, VIC 3000 ("**FrankieOne**").

(Client and FrankieOne together are "**the Parties**" and separately, "**a Party**".)

BACKGROUND AND CONSTRUCTION OF DPA:

A. The Parties enter into this DPA with respect to Personal Data regulated under Data Protection Law and:

   (1) that is provided to FrankieOne by or on behalf of Client and which is Processed by FrankieOne as Processor;

   (2) that is exchanged between the Parties on a Controller to Controller basis;

   (3) that is subject to the GDPR, Swiss law or United Kingdom law and is transferred, directly or via onward transfer, to a Party who is located outside any member state of the European Economic Area ("**EEA**"), Switzerland, or the United Kingdom.

B. Capitalized terms used in this DPA shall have the meaning given to them in Section 5 (Definitions), unless otherwise specified.

C. The terms in this DPA shall be incorporated into and form part of the agreement between Client and FrankieOne governing Client's use of FrankieOne's software-as-a-service and incorporated online services ("**Agreement**"), and the Agreement and this DPA shall be read as one document.

D. This DPA does not need to be separately executed by the Parties if the DPA is already explicitly incorporated into a fully executed Agreement, in which case the Parties' signature to that Agreement shall be deemed proper signature of this DPA. In the event of conflict with any other terms of the Agreement, this DPA shall prevail.

E. In the event that Data Protection Laws are amended, replaced or repealed, the Parties shall, where necessary, negotiate in good faith a solution to enable the transfer of Personal Data to be conducted in compliance with Data Protection Laws.

F. This DPA sets out the obligations of the Parties in relation to the Processing of Personal Data.

1. CONTROLLER TO PROCESSOR RELATIONSHIP

(a) Client acts as Controller and FrankieOne acts as a Processor when Processing any Personal Data contained in Client Data provided to FrankieOne by Client (or its customers) for the purposes of FrankieOne providing a software-as-a-service subscription or any other service to Client under an Agreement, or otherwise complying with its obligations (collectively the "**Services**"). In these circumstances, FrankieOne will:

   (i) process the Personal Data on behalf of Client solely in accordance with the Agreement, this DPA, Client's written instructions (if any), and applicable Data Protection Laws. If FrankieOne is legally required to process Personal Data otherwise

than as instructed by Client, it will notify Client before such processing occurs, unless the law requiring such processing prohibits FrankieOne from notifying Client;

(ii) not collect, retain, use or disclose the Personal Data for any other purpose. For the avoidance of any doubt, Client instructs FrankieOne to Process the Personal Data as reasonably necessary and proportionate to achieve FrankieOne's business purposes to the extent permitted by applicable Data Protection Laws; and

(iii) not combine the Personal Data it receives from, or on behalf of, Client with Personal Data it receives from, or on behalf of, another person or persons, or collects from its own interaction with a data subject, unless permitted by the applicable Data Protection Laws.

Details of this Processing are set out in Schedule 1 attached to this Addendum.

(b) FrankieOne further agrees that it will, to the extent required by applicable Data Protection Laws when acting as a Processor in the provision of the Services:

(i) inform Client if any instruction provided by it contradicts any legal requirements to which FrankieOne is subject;

(ii) keep all Personal Data confidential as required under the Agreement and ensure that persons authorised by FrankieOne to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii) provide access to Personal Data only to those of its employees, related bodies corporate or Subprocessors who need access to such data for the purposes set out in Section 1(a);

(iv) take appropriate technical and organizational security measures designed to safeguard Personal Data against unauthorised access, destruction, disclosure, transfer, or other improper use as set forth in Schedule 2 attached to this DPA;

(v) provide Client with a means to access Personal Data of Data Subjects, which have been provided by Client to FrankieOne, to enable Client to comply with its obligations to Data Subjects exercising their rights under Data Protection Laws. This may include FrankieOne providing the Client with the ability to directly amend, correct, delete, add to, cease using or restrict the use of Personal Data relating to such Data Subjects through the Services;

(vi) promptly notify Client of any accidental or unauthorised access, destruction, disclosure, transfer of Personal Data that have been supplied by Client, after FrankieOne becomes aware of any such access, destruction, disclosure, transfer or other improper use, or of any complaints by individuals or third parties that involve or pertain to such Personal Data, and shall, taking into account the nature of the Processing and the information available to FrankieOne, provide such assistance to Client as may be reasonable in the circumstances to enable Client meet its obligations to notify any Supervisory Authority or any other regulatory or governmental authorities or Data Subjects of such event where Client is required to do so by law;

(vii) taking into account the nature of the Processing and the information available to FrankieOne, use reasonable endeavours to assist Client in relation to any privacy impact assessments or consultations with Supervisory Authorities about the Processing of Personal Data in the context of the provision of the Services or any inquiry, complaint or claim in relation to the Processing by FrankieOne of Personal

Data provided by Client;

(viii) allow Client the right to take reasonable and appropriate steps to ensure that FrankieOne is using the Personal Data in a manner consistent with Client's obligations under the applicable Data Protection Laws, by allowing Client to audit FrankieOne by receiving reasonably reliable documentation regarding the adequacy of the Processing by the FrankieOne of Personal Data on behalf of the Client. Such documentation may include:

1. an annual SOC2 (or subsequent successor) audit of FrankieOne's available security policies and procedures;
2. certification of ISO 27001 standards or such alternative standards that are substantially equivalent to ISO 27001; or
3. otherwise provide for demonstrable assurances of data processing facilities used by FrankieOne to Process Personal Data on behalf of the Client, including penetration tests or vulnerability scans ("**Audit Report**").

Unless otherwise required by a Supervisory Authority or mutually agreed by the Parties in writing, any audit of FrankieOne shall be limited to the provision of the Audit Report;

(ix) at the expiry of termination of the Agreement or this DPA, at Client's election, delete or return the Personal Data to Client, provided that Client acknowledges and agrees that any Personal Data stored within the Services as provided by Client to FrankieOne shall be deleted either as specified within the Agreement or, if the Agreement is silent, within sixty (60) days of termination of the Agreement;

(x) the Client acknowledges and agrees that FrankieOne may retain third parties as Subprocessors in connection with this DPA, having imposed on such Subprocessors substantially similar data protection obligations as are imposed on FrankieOne under this DPA. At all times, FrankieOne remains responsible and liable for Subprocessor acts and omissions. A list of relevant Subprocessors to the Services has been attached at Schedule 3.

In the event FrankieOne adds or replaces a Subprocessor for the Services, Client may object to the use of a new Subprocessor by sending a notification to privacy@frankieone.com within ten (10) business days of receipt of notice of a new Subprocessor provided that the Client reasonably believes that use of such Subprocessor presents an unreasonable risk to or prevents the Client from complying with applicable law. If Client so objects, FrankieOne shall either:

1. not use the new Subprocessor to process the Client Personal Data; or
2. shall find an alternative way of reasonably resolving Client's objection.

If neither (a) nor (b) is reasonably feasible within thirty (30) days of receipt of Client's objection, then Client shall either rescind its objection or may terminate any services for which the new Subprocessor would be used by providing written notice to FrankieOne at the address for notices indicated in the Agreement or this Addendum. For the avoidance of doubt, in the event Client does not object to a new Subprocessor in accordance with this Section, Client shall be deemed to have consented to the new Subprocessor.

(c) To the extent that the provision of the Services under this Section 1 involves the transfer of Personal Data that is subject to the GDPR, Swiss law, or United Kingdom law by Client (as Data Exporter) to FrankieOne (as Data Importer), the Parties agree to either:

(i) comply with the terms of Module 2 of the Transfer Clauses (where Client acts as a Controller) or Module 3 of the Transfer Clauses (where Client acts as a Processor retaining FrankieOne as an additional Processor), which Transfer Clauses are incorporated herein by reference; or

(ii) otherwise Process such Personal Data using a valid transfer mechanism in accordance with Data Protection Laws.

2. CONTROLLER TO CONTROLLER RELATIONSHIP

(a) Section 1 does not apply where Vendor is acting as a Controller of Personal Data.

(b) To the extent that FrankieOne Processes Personal Data provided to it by Client for purposes other than as set forth in Section 1(a) above, which is specified in FrankieOne's Privacy Policy, FrankieOne acknowledges that it will be a Controller of that Personal Data, and FrankieOne agrees to Process such Personal Data in accordance with Data Protection Laws.

3. CLIENT OBLIGATIONS

In relation to all Personal Data provided by Client to FrankieOne for Processing under the Agreement, Client shall ensure that:

(a) all relevant Data Subject have consented (in accordance with applicable Data Protection Laws) to their Personal Data being disclosed to FrankieOne for Processing in accordance with the Agreement and this DPA;

(b) notice of the disclosure of Personal Data to FrankieOne for Processing in accordance with this Agreement and DPA will be provided to all relevant Data Subjects (including users of the Services) prior to any disclosure and, where requested by FrankieOne, Client shall provide evidence that it has provided such notice;

(c) Client complies with and warrants that it has complied with applicable Data Protection Laws in relation to the disclosure of Personal Data to FrankieOne, including that disclosure was in any and all cases lawful; and

(d) it shall not, by any act or omission, put FrankieOne or any of its related bodies corporate in breach of any applicable Data Protection Laws.

4. TRANSFER CLAUSES

(a) Where the Transfer Clauses apply under this DPA:

(i) the Parties elect to add the optional Clause 7 (Docking Clause) of the Transfer Clauses;

(ii) the Parties do not elect to add the additional optional language under Clause 11(a) (Redress) of the Transfer Clauses;

(iii) for the purposes of Clause 17 (Governing Law) of the Transfer Clauses, the Parties elect Option 1, and the Parties agree that this shall be the law of Ireland;

(iv) for the purposes of Clause 18 (Choice of Forum and Jurisdiction) of the Transfer Clauses, the Parties agree that any dispute arising from these Clauses shall be resolved by the Courts of Ireland;

(v) the Parties' signature to this DPA or Agreement that explicitly incorporates this DPA shall be considered a signature to the Transfer Clauses, and if so required by the

laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the Transfer Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required; and

(vi) in the event that the Transfer Clauses are amended, replaced or otherwise invalidated by the European Commission or under the Data Protection Laws, the Parties shall work together in good faith to enter into any updated version of such Transfer Clauses or negotiate in good faith a solution to enable a transfer of the Personal Data to meet the requirements of applicable Data Protection Laws.

(b) With respect to Module 1 of the Transfer Clauses, Schedule 1 of this DPA shall serve as Annex I of the Transfer Clauses.

(c) With respect to Modules 2 and 3 of the Transfer Clauses, the following additional provisions shall apply:

(i) Schedules 1 and 2 of this DPA shall serve as Annexes I and II respectively of the Transfer Clauses;

(ii) the Parties agree that any audits described in Clause 8.9 of the Transfer Clauses shall be carried out in accordance with Section 1(b)(viii) of this DPA;

(iii) for purposes of Clause 8.6(c) and (d) (Security of Processing) of Module 3 of the Transfer Clauses, where Client acts as Processor, the Parties acknowledge and agree that it will not be appropriate and feasible for FrankieOne to directly notify the Controller of a Personal Data Breach concerning Personal Data Processed by Vendor under the Transfer Clauses, and Client agrees to forward to the Controller any such notification of a Personal Data Breach without undue delay;

(iv) for purposes of Clause 8.9 (Documentation and Compliance) of Module 3 of the Transfer Clauses, where Client acts as Processor, Client agrees that all inquiries from the Controller shall be provided to FrankieOne by the Client (for and on behalf of the Controller) and, except as determined necessary by FrankieOne to ensure that inquiries are promptly and adequately be dealt with, all relevant communication shall be handled solely via the Client. In case FrankieOne receives an inquiry directly from the Controller, it shall promptly forward the inquiry to the Client;

(v) for the purposes of Clause 9(a) (Subprocessors) of the Transfer Clauses, the Parties elect Option 2 (General Written Authorisation). It is understood and agreed that the Client provides the general authorisation and instruction for the engagement of the Subprocessors from the list in Schedule 3 of this DPA and the Parties agree to observe the provisions set out in Section 1(b)(x) of this DPA in relation to additions or replacements of Subprocessors.

Where the Client acts as a Processor under Module 3, the Client:
warrants that it has the authority to provide general authorisation and instruction on behalf of the Controller; and
agrees to inform the Controller of any addition or replacement of Subprocessors from the agreed list in Schedule 3 of this DPA on behalf of FrankieOne, to enable FrankieOne to comply with its obligations under Clause 9(a) the Transfer Clauses; and

(vi) for the purposes of Clause 10 of Module 3 (Data Subject Rights) of the Transfer Clauses, where Client acts as Processor, the Parties acknowledge and agree that it will not be appropriate for FrankieOne to directly notify the Controller of any request it has received from a Data Subject, and Client agrees to promptly forward to the

Controller any such notification and to be primarily responsible to assist the Controller in fulfilling the relevant obligations to respond to any such request;

(vii) for the purposes of Clause 13 of the Transfer Clauses, the competent supervisory authority shall be the supervisory authority identified by Client on the signature page of this DPA or, if Client does not so identify a competent supervisory authority, the competent supervisory authority shall be the supervisory authority of the Member State in which the data exporter is established or has appointed a representative pursuant to Article 27(1) of the GDPR, and such competent supervisory authority shall be incorporated into Annex I.C of the Transfer Clauses.

(d) For transfers of Personal Data that are subject to the Data Protection Laws of the United Kingdom, the Transfer Clauses are amended and subject to the following provisions:

(i) Part 2: Mandatory Clauses of the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses applies; and

(ii) the information required by Part 1 of the Approved Addendum is set out at Schedule 1-4 of this Addendum (as applicable).

(e) For transfers of Personal Information that are subject to the Data Protections Laws of Switzerland, the Transfer Clauses are amended and subject to the following provisions:

(i) the term “EU Member State” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with the Transfer Clauses;

(ii) the Federal Data Protection and Information Commissioner shall act as the “competent supervisory authority” insofar as the relevant data transfer is governed by the Swiss Federal Act on Data Protection;

(iii) the Transfer Clauses shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

5. GOVERNING LAW

Except for the Transfer Clauses, this DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed in all respects by, and construed in accordance with, the governing law of the original Agreement executed between the Parties.

6. DEFINITIONS AND INTERPRETATION

For the purposes of interpreting this DPA:

(a) Agreement has the meaning defined in Section C of Background and Construction of this DPA;

(b) Audit Report has the meaning defined in Section 1(b)(viii) of this DPA;

(c) Client is the entity defined on the execution page of this DPA;

(d) Client Data means all data submitted, provided, entered, or stored by the Client within FrankieOne’s Services or software-as-a-service offering, which the Client has access to or

has otherwise purchased;

(e) the terms "Controller", "Personal Data Breach", “Processor”, "Process(ing)", and "Data Subject", with respect to Personal Data subject to the GDPR, each have the meaning given to such terms in the GDPR, and with respect to all other Personal Data, “Controller” means the entity responsible for deciding the purpose and means for Processing Personal Data and “Processor” means the entity that Processes Personal Data on behalf of the Controller;

(f) Data Protection Laws means any applicable laws, regulations, or other binding obligations (including any and all legislative and/or regulatory amendments or successors thereto), each as updated from time to time, of the European Union, the EEA, Switzerland, the United Kingdom, Australia or any other jurisdiction that govern or otherwise apply to Personal Data Processed under the Agreement;

(g) DPA means this Data Processing Addendum;

(h) EEA means European Economic Area;

(i) GDPR means European Union Regulation 2016/679 and includes any relevant implementing measure in each relevant Member State, or any successor legislation thereto;

(j) FrankieOne means Frankie Financial Pty Ltd as detailed on the first page of this DPA;

(k) Party/Parties has the meaning defined on the first page of this DPA;

(l) Personal Data means any information that relates to, identifies, describes, is capable of being associated with, or could reasonably be linked to, directly or indirectly, an identified or identifiable natural person or individual. This can include identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person and to the extent applicable under relevant Data Protection Laws, an identified or identifiably household;

(m) Related bodies corporate has the definition under Section 50 of the Corporations Act 2001 (Cth), an Australian legislation;

(n) Services has the meaning defined in Section 1(a) of this DPA;

(o) Subprocessor means a Processor appointed by FrankieOne to assist with the provision of the Services to the Client or the performance of FrankieOne’s obligations under the Agreement, which is set out in Schedule 3;

(p) Supervisory Authority means the data protection authority in the applicable Member State of the European Union and the equivalent authorities in each other state within the EEA, Switzerland, the United Kingdom or any other jurisdiction whose Data Protection Laws apply to the Processing of the Personal Data subject to this DPA; and

(q) Transfer Clauses means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR.

frankieone

EXECUTED AS AN AGREEMENT

The Parties, each acting under due and proper authority, have executed this DPA as of the date of last signature. The Parties agree that execution of this Addendum via an electronic signature process shall constitute valid execution.

Client

Client Name: _____

Signature: _____

Signatory Name: _____

Title: _____

Date: _____

Address: _____

_____

Contact Person's Name: _____

Contact Person's Position_____

Contact Person's Address: _____

_____

FrankieOne

Frankie Financial Pty Ltd

Signature: Signed by: Jacqueline Tan 9F7C1FE82306B85C

Signatory Name: Jacqueline Tan

Title: CFO

Date: 26/08/2026

Address: Level 6, 440 Collins St, Melbourne VIC 3000

frankieone

SCHEDULE 1 – DETAILS OF THE PROCESSING ACTIVITIES

Annex I – Modules 2 and 3

This Schedule 1 forms part of the DPA and also serves as Annex I to Modules 2 and/or 3 of the Transfer Clauses.

A. List of Parties

Data Exporter

Name: the Client identified on the signature page of the DPA or in the Agreement that explicitly incorporates this DPA.

Address: as identified on the signature page of the DPA or in the Agreement that explicitly incorporates this DPA.

Contact person's name, position and contact details: as identified on the signature page of the DPA or in the Agreement that explicitly incorporates this DPA.

Activities relevant to the data transferred under Modules 2 and/or 3: Client shall be providing Personal Data as necessary to receive the Services and as FrankieOne is further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws and Regulations, to achieve FrankieOne's business purposes.

Role: Controller or Processor (as appropriate)

Data Importer

Name: FrankieOne

Address: as identified on the first page of the DPA or in the Agreement that explicitly incorporates this DPA.

Contact person's name, position and contact details: Adonis Kaddour, Data Protection Officer, privacy@frankieone.com

Activities relevant to the data transferred under Modules 2 and/or 3: FrankieOne shall Process Personal Data as necessary to perform the Services and as further instructed by Client, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws and Regulations, to achieve FrankieOne's business purposes.

Role: Processor

B. Description of the Processing and Transfer

Categories of Data Subjects
Client may submit Personal Data to FrankieOne, the extent of which is determined and controlled by the Client in its discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Client's customers, business partners, vendors, and other third parties of Client, employees, directors, officers, contact persons, and users authorised to use FrankieOne's services.

Categories of Personal Data
The Client may submit special categories of data to FrankieOne, the extent of which is determined and controlled by Client in its sole discretion. Categories of Personal Data may include first name, last name, sign-in credentials, email address, username and password, contact information, ID documents, IT information (IP addresses, usage data, cookies data, location data, browser data), device information (web browser type, operating system version, mobile device model, device manufacturer and model, language and regional settings, your Internet Service Provider (ISP), unique

device identifiers), financial information (credit card details, bank account details, payment information), employment details (employer, job title, geographic location, area of responsibility) and any other Personal Data of the type necessary to enable the Processor to provide the Services.

Special Categories of Sensitive Data
The Client may submit special categories of data to FrankieOne, the extent of which is determined and controlled by Client in its sole discretion. This may include: Biometric data, including facial images and derived biometric templates, processed through facial matching and liveness detection technologies for the sole purpose of verifying that an individual is the legitimate holder of an identity document and preventing fraud.

Frequency of Transfer
The Personal Data is transferred on a continuous basis for as long as Client has an active Service accessed or purchased, unless otherwise agreed between the Parties.

Nature of the Processing
FrankieOne will Process Personal Data as necessary to perform the Services pursuant to the Agreement and this DPA on behalf of the Client, and as further instructed by Client in writing in its use of the Services, specifically including Processing as reasonably necessary and proportionate and, to the extent such Processing by Processors is permitted by Data Protection Laws, to achieve FrankieOne's business purposes

Purposes of the Data Transfer and Processing
The purpose of the data transfer and processing is to fulfil the objectives of the Agreement between the Parties and deliver Services as contemplated by such Agreement. Any Special Categories of Sensitive Data is not processed for profiling, tracking, or identification of individuals outside the relevant verification transaction, and is not used to create persistent biometric identifiers.

Period of Retention
For the duration as set out directly below and as otherwise agreed between the Parties in writing (including in this DPA).

Subject Matter of Processing
The subject matter of the Processing is enabling the Client to receive the value of the Services as contemplated under this DPA and the Agreement, including enabling FrankieOne to deliver support, customer success, and the Services, including enabling the security of Services. Client Data is hosted and stored in Australia, and Transfer Clauses apply.

Duration
For the duration of the Services and any agreed period in writing for retention upon termination of the Services until deletion.

frankieone

SCHEDULE 2 – TECHNICAL AND ORGANISATIONAL MEASURES

This Schedule forms part of the DPA and serves as Annex II of the Transfer Clauses.

The following is a description of the technical and organisational measures implemented by FrankieOne to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

1. Access control to premises and facilities
Measures taken to prevent unauthorised physical access to premises and facilities holding personal data shall include:

- Covered by FrankieOne's ISO 27001:2022 and SOC2 Type II compliance and audit programmes.
- Physical presence and storage of Personal Data is outsourced to Amazon Web Services (see Sub-processors)
- AWS provide physical security of datacentres in-line with their Shared-Responsibility model. See https://aws.amazon.com/compliance/ for more

2. Access control to systems
Measures taken to prevent unauthorised access to IT systems include the following technical and organisational measures for user identification and authentication:

- Covered by FrankieOne's ISO 27001:2022 and SOC2 Type II compliance and audit programmes.
- Strict access control measures across all systems within FrankieOne's control
- Strong password and MFA policies & procedures
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data
Measures taken to prevent authorised users from accessing data beyond their authorised access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data include:

- All data is encrypted in application with unique keys bound to the customer
- All data is also separately encrypted in transit and at rest using strong encryption protocols
- Access to data is strictly controlled with fine-grained access controls that are monitored and audited regularly
- System control measures in place to prevent unauthorised services from being deployed with end-to-end analysis and monitoring to the entire platform

4. Disclosure control
Measures taken to prevent the unauthorised access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Creating an audit trail of data transfers

5. Input control
Measures put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained include:

- Logging user activities on IT systems
- Ability to verify and establish to which bodies have access to personal data

- Ability to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input

6. Job control
Measures put in place to ensure that data is processed strictly in compliance with the data importer's instructions include:

- No deployment of service changes without clear sign-off from data importer/owner
- Unambiguous wording of contractual instructions
- Monitoring of contract performance
- Regular configuration and performance review

7. Availability control
Measures put in place designed to ensure that data are protected against accidental destruction or loss include:

- Installed systems may, in the case of interruption, be restored
- Systems are functioning, and that faults are reported
- Stored personal data cannot be corrupted by means of a malfunctioning of the system
- Multiple redundant sites and services to provide high availability in all cases
- Business Continuity procedures
- Remote real-time backups
- Anti-virus/firewall systems

8. Segregation control
Measures put in place to allow data collected for different purposes to be processed separately include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

frankieone

SCHEDULE 3 – LIST OF SUBPROCESSORS

Subprocessors engaged in the Processing of Personal Data, where the Client is the Controller, in connection with FrankieOne's provision of Services includes the following entities, as outlined.

Sub-Processor	Country	Purpose	Contact details
Amazon Web Services	AUS	Cloud-based web hosting	https://aws.amazon.com/compliance/gdpr-center/
Cloudflare	Global	System border security, (D)DoS Protection, Global CDN	https://www.cloudflare.com/gdpr/introduction/ https://www.cloudflare.com/trust-hub/
Google	Global	Email, Calendar, Document Management, SSO	https://cloud.google.com/privacy/gdpr https://workspace.google.com/security/
Atlassian	US	Technical project management, task tracking, supporting ticketing	We use Jira for our ticketing and task management and Confluence for our internal knowledge base. No customer data is stored in any of the Atlassian products in use. https://www.atlassian.com/trust/privacy/gdpr https://www.atlassian.com/trust
HubSpot	US	CRM, marketing automation, and customer engagement	https://legal.hubspot.com/gdpr https://security.hubspot.com/
Rippling	US	HR, payroll, and employee lifecycle management	https://www.rippling.com/gdpr https://www.rippling.com/security
Trelica	EU	Internal User Management	https://legal.trelica.com/security-practices https://legal.trelica.com/privacy-policy
Slack	US	Communication and collaboration	https://slack.com/trust/compliance/gdpr https://slack.com/trust/security
Xero	AU	General accounting, payroll processing and employee compensation management	https://www.xero.com/au/about/terms/privacy/gdpr/ https://www.xero.com/au/security/
Annature	AUS	Document signing	https://www.annature.com.au/privacy-policy

Appcues	US	In-portal feature management	https://trust.appcues.com/
SuprSend	US, EU	In-portal messaging and notifications	https://trust.suprsend.com/ https://www.suprsend.com/privacy
ThoughtSpot	US	Data Analytics	https://www.thoughtspot.com/legal/gdpr-compliance
Twilio	US	SMS Messaging	https://www.twilio.com/en-us/gdpr
Hotjar	US	Portal usage analytics	https://help.hotjar.com/hc/en-us/sections/35766918492433
ArangoDB	AU - AWS Sydney	Graph Database	We use ArangoDB as our graph database for mapping business ownership and fraud connectivity data. No PII is kept in this database.
Uptycs	US	CNAPP	We use Uptycs to monitor our code and platform for security issues.