DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("DPA") forms part of the iplicit Software Services Subscription Agreement ("Agreement") entered into between **Customer** ("Controller") and **iplicit** ("Processor"). This DPA sets out the terms and conditions governing the Processing of Personal Data by the Parties and is intended to ensure such Processing is conducted in accordance with applicable Data Protection Legislation.

In any event of any conflict between the terms of this DPA and the Agreement, the terms of this DPA shall prevail with respect to the processing of Personal Data.

1. DEFINITIONS

1.1. In this DPA, the following shall have the meanings set out below. Capitalised terms used and not defined in this SLA will have the meanings set forth in the Agreement.

"Data Protection Legislation" means, as applicable:

- **"UK Data Protection Laws"**: The UK GDPR as defined in section 3(10) of the Data Protection Act 2018, and the Data Protection Act 2018 itself.

- **"EU Data Protection Laws"**: Regulation (EU) 2016/679 ("EU GDPR") and any applicable national implementing laws.

"**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" (and "**Process**"), "**Processor**", and "**Supervisory Authority**" shall have the meanings given to them in the EU GDPR or UK GDPR.

"Restricted Transfer" means a transfer of Personal Data which is prohibited by Data Protection Legislation in the absence of a specific safeguard (such as the Standard Contractual Clauses).

"Standard Contractual Clauses" (SCCs) means the contractual clauses adopted by the European Commission (Decision 2021/914) for the transfer of personal data to third countries.

"UK Addendum" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner (Version B1.0).

2. SCOPE AND ROLES

2.1. **Roles:** The Customer is the Controller and iplicit is the Processor. If the Customer is acting as a Processor for others, iplicit is a sub-processor.

2.2. **Processing:** iplicit shall process Personal Data only for the "Business Purposes" (providing the Software/Services described in the Agreement) and in accordance with the Controller's written instructions unless required by UK/EU law, in which case Processor will inform Controller before processing. If Processor believes a Controller instruction infringes Data Protection Law, it shall inform Controller.

3. SECURITY AND CONFIDENTIALITY

3.1. **Measures:** iplicit shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, specifically addressing the risks of accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of data.

3.2. **Confidentiality:** iplicit ensures that persons authorised to process the Personal Data (employees) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. SUB-PROCESSORS

4.1. **General Authorisation:** The Controller grants iplicit a general written authorisation to engage sub-processors (including, but not limited to, cloud infrastructure providers) to provide the Services.

4.2. **New Sub-processors:** iplicit will notify the Controller of any intended changes concerning the addition or replacement of sub-processors. The Controller may reasonably object to such changes in writing within 30 days on commercially reasonable data protection grounds.

4.3. **Objection:** If the parties cannot agree on a resolution to the objection, the Parties will agree to work together to find a mutually acceptable workaround, not to be unreasonably withheld or rejected. Failing to find a mutually acceptable workaround, either party may terminate the specific part of the Service affected by the sub-processor. iplicit shall ensure that any sub-processor is bound by data protection obligations no less protective than those set out in this DPA, as required by Article 28(4).

4.4. **Liability:** iplicit remains fully liable to the Controller for the performance of the sub-processor's data protection obligations.

5. INTERNATIONAL DATA TRANSFERS

5.1. **UK/EU Adequacy:** Transfers between the United Kingdom and the European Economic Area (EEA) are currently permitted under the respective "Adequacy Decisions" of the UK Government and the European Commission.

5.2. **Restricted Transfers:** If iplicit transfers data to a country without an Adequacy Decision (a "Restricted Transfer"), the following safeguards apply:

- **EU Data:** The EU Standard Contractual Clauses (Module 2 or 3 as applicable) shall apply.
- **UK Data:** The UK Addendum to the EU SCCs shall apply. 5.3. By signing this DPA, the parties agree that these safeguards are incorporated by reference where required by law.

6. ASSISTANCE TO CONTROLLER

6.1. **Data Subject Rights:** iplicit shall provide reasonable assistance (via technical and organisational measures) to enable the Controller to respond to Data Subject Requests (e.g., access, deletion). iplicit shall not respond directly to a Data Subject unless authorised.

6.2. **DPIAs:** iplicit shall provide reasonable assistance to the Controller with Data Protection Impact Assessments (DPIAs) and prior consultations with Supervisory Authorities, limited to the nature of processing and information available to iplicit.

6.3. Additional Assistance: Where the Controller requests assistance from iplicit in relation to Data Subject Rights or Data Protection Impact Assessments (DPIAs) that goes beyond the reasonable technical and organisational measures described in this Agreement, iplicit may charge the Controller for such additional assistance at its then-current professional services rates, provided that iplicit obtains the Controller's prior written consent before incurring any such charges.

7. DATA BREACH NOTIFICATION

7.1. **Notification:** iplicit shall notify the Controller without undue delay (and in any event within 24 to 48 hours) after becoming aware of a Personal Data Breach.

7.2. **Content:** The notification shall describe the nature of the breach, likely consequences, and measures taken to mitigate it.

7.3. **Control:** The Controller retains the sole right to determine whether to notify the Data Subjects or the Regulator (Information Commissioner).

8. AUDIT AND RECORDS

8.1. **Records:** iplicit shall maintain records of processing activities as required by Article 30 of the GDPR. Processor shall make available to Controller all information necessary to demonstrate compliance with this DPA and Article 28, and allow for and contribute to audits.

8.2. **Audit Rights:** The Controller may remote audit iplicit's compliance with this DPA up to once per year, upon 30 days' prior written notice.

8.4. **Costs:** If the Controller requests assistance or undertakes its Audits Rights, iplicit reserves the right to charge for such time at agreed professional services rates.

9. DELETION OR RETURN

9.1. Upon termination of the Agreement, iplicit shall (at the Controller's choice) delete or return all Personal Data, unless applicable law requires its retention.

10. LIABILITY AND INDEMNITY

10.1 Liability Cap. The total aggregate liability of each party under this DPA and in respect of the processing of Customer Personal Data shall be subject to the same limitations and exclusions of liability as set out in the Agreement. For the avoidance of doubt, nothing in this DPA shall increase or expand either party's liability beyond the limitations agreed in the Agreement, and any remedies or damages awarded under this DPA will count toward and not exceed those limitations.

7.2 Indemnity. Processor shall indemnify and hold harmless Controller against any fines, claims, damages or losses finally awarded by a court or regulator, or agreed in settlement with Processor's consent, to the extent arising from Processor's breach of its obligations under this DPA or applicable Data Protection Law. Controller shall likewise indemnify and hold harmless Processor against any third-party claims or regulatory fines to the extent arising from Controller's instructions or actions that violate Data Protection Law. Each party's liability under this indemnity is subject to the limitations in Clause 10.1 (Liability Cap) above.

7.3 Exclusions. Neither party shall be liable to the other for any indirect or consequential losses, or any loss of profit, revenue, goodwill, or data, arising under this DPA, in accordance with the Agreement.

7.4 GDPR Responsibilities. Notwithstanding the foregoing, the parties acknowledge that nothing in this DPA relieves either party of any liability it may incur vis-à-vis data subjects or regulators under UK or EU GDPR. Controller remains fully responsible for complying with its obligations as Controller, and Processor for its obligations as Processor, under applicable law. This clause 10 (Liability and Indemnity) governs the allocation of risk as between the parties only.

11. TERM AND TERMINATION

11.1 This DPA shall commence on the Effective Date and shall continue in full force and effect for so long as Agreement is in effect (the "**Term**").

11.2. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Agreement to protect the Personal Data will remain in full force and effect.

11.3. If a change in any Applicable Data Protection Law prevents a Party from fulfilling its obligations, the Parties shall negotiate in good faith to amend this DPA.

APPENDIX A: DETAILS OF PROCESSING

1. Subject Matter Personal data is processed for the performance the Agreement in the provision of the iplicit cloud accounting and finance software services as described in the Agreement.

2. Duration For the term of the Agreement and any subsequent period required for data retention, return, or deletion as set out in the Agreement and this DPA.

3. Nature and Purpose collection, storage and making available data collected by Controller to manage the performance of the Agreement and that data inputted into the Controller's platform by Controller or their Authorised Users.

4. Data Categories The Personal Data transferred concerns the following categories of data:

- **Identity Data:** Names, usernames, and professional contact details (email, telephone, address).
- **Financial Data:** Transactional records, invoices, expenses, bank account details, and payment history.
- **Employment Data:** Payroll and employee records (where applicable to the modules purchased).
- **Technical Data:** User login credentials, IP addresses, system audit logs, and usage metadata.

There may be other categories of Personal Data, to the extent the Controller of their Authorised Users inputs Personal Data into the 'free fields' elements of the Software.

5. Data Subjects The Personal Data transferred concerns the following categories of data subjects:

- Employees, agents, Authorised Users and contractors of the Controller.
- Customers and suppliers of the Controller or any person inputted into the Software by the Controller and its Authorised Users.

6. Approved Sub-processors

The Controller acknowledges and authorises the engagement of the following Sub-processors:

COMPANY NAME	LEGAL ENTITY	DATA LOCATION	SERVICES PROVIDED	US DATA PRIVACY FRAMEWORK
Microsoft Azure	Microsoft UK Ltd Microsoft Campus, Thames Valley Park, Reading, Berkshire, RG6 1WG	UK (EU – Dublin and Netherlands on request)	Cloud hosting and file storage	Yes

Exchange online (Outlook)	Microsoft UK Ltd Microsoft Campus, Thames Valley Park, Reading, Berkshire, RG6 1WG	UK	Exchange Online, also known as Outlook, is a hosted messaging application that provides organisations with access to the full capabilities of Exchange Server with the flexibility and scalability of cloud-based infrastructure.	Yes
Microsoft Office 365/SharePoint/Teams/Portal Access	Microsoft UK Ltd Microsoft Campus, Thames Valley Park, Reading, Berkshire, RG6 1WG	UK	Office 365, incorporating SharePoint and Portal Access, is a comprehensive suite of cloud-based productivity and collaboration tools that enhances team efficiency and streamlines enterprise content management and communication	Yes
Hubspot	HubSpot Inc. Two Canal Park, Cambridge, MA 02141	US	Customer Relationship Management software	Yes
Freshdesk	Freshworks, Inc. San Mateo, California	US	Helpdesk & Support services	Yes
Zapier	Zapier Inc. 548 Market St PMB 62411, San Francisco, CA 94104	US	Web application integration and workflow automation	Yes
LearnUpon	LearnUpon Limited. Dublin, Ireland.	EU	Learning Management System	N/A
MailGun	Mailgun Technologies, Inc. 21750 Hardy Oak Blvd, Suite 104, San Antonio, TX 78258	EU	Used to receive emails for AP Automation and handles sending of emails for MTD portal	Yes
Teamwork	Teamwork Crew Limited Teamwork Campus 1, Park House Blackpool Retail Park Cork T23 AX73 Ireland	EU	Customer Services project management tool to manage customer implementations	Yes
Yapily	Yapily Ltd. registered in England and Wales with the company number 10842280.	UK or EU	Open Banking Gateways Customer agrees to Yapily terms via iplicit prior to utilisation	N/A
Yodlee	Yodlee, Inc. Redwood City, California.	EU, US	Open Banking Gateways Customer agrees to Yodlee terms via iplicit prior to utilisation	N/A
LightYear			Automated Accounts Payable	N/A

	Lightyear UK Ltd. 256-260 Old Street, London EC1V 9DD, United Kingdom.	AWS Oregon, images stored in Ire or Aus	Customer agrees to LightYear terms via iplicit portal prior to utilisation	
Cin7	Cin7 UK Limited 10 John Street London WC1N 2EB	UK/Global (processing based on entity)	Inventory Management, Order processing and payments Customer agrees to Cin7 T&Cs to get the requisite license	N/A
GoCardless	GoCardless Ltd Suton Yard 65 Goswell Road London EC1V 7EN	UK	Open Banking Gateways (Payment Initiation Services) Customer agrees to Plaid terms prior to utilisation	N/A
Plaid	Plaid Financial Limited New Penderel House 4th Floor, 283-288 High Holborn WC1V 7HP	UK/EU (Open Banking Data)	Open Banking Gateways (Payment Initiation Services) Customer agrees to Plaid terms via iplicit prior to utilisation	N/A
Crezco	Crezco Limited 192 Campden Hill Road London W8 7TH	UK and/or EEA	Authorised Payment Institution (API); Open Banking Gateways (PIS/AIS); B2B Payables Automation Customer agrees to Crezco terms via iplicit prior to utilisation	N/A

APPENDIX B: TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

1. Certifications and Standards

- **ISO/IEC 27001:2022:** The Processor maintains a full Information Security Management System (ISMS) certified against the ISO/IEC 27001:2022 standard.
- **ISO 9001:2015:** The Processor maintains a Quality Management System certified against ISO 9001:2015.
- **UK FCA:** The Processor is registered with the Financial Conduct Authority as an Account Information Service Provider (AISP).

2. Physical and Environmental Security

- **Cloud Infrastructure:** The Service is hosted exclusively on Microsoft Azure. Physical security controls (power, cooling, physical access) are managed by Microsoft under the Shared Responsibility Model.
- **Data Residency:** Customer data is processed and stored exclusively within the Customer's chosen geographical region (UK or EU).

3. Identity and Access Management (IAM)

- **Customer Authentication:** The Service supports Single Sign-On (SSO) via SAML 2.0 and Microsoft Entra ID (formerly Azure AD). Multi-Factor Authentication (MFA) is supported.
- **Internal Privileged Access:** The Processor operates a Zero Trust model. Engineers have no standing access to production data. Access is granted via Just-In-Time (JIT) requests using Azure Privileged Identity Management (PIM), which are time-bound, audited, and require MFA.

4. Network and Operations Security

- **Perimeter Defence:** All ingress traffic is routed through Azure Front Door, utilising a Web Application Firewall (WAF) configured to block OWASP Top 10 threats (e.g., SQL Injection, XSS) and perform DDoS mitigation.
- **Network Isolation:** Production environments reside in isolated Azure Virtual Networks (VNet). Traffic between application and database layers travels via Azure Private Link, avoiding the public internet.
- **Monitoring:** The environment is monitored 24/7 using Microsoft Sentinel (SIEM) and Microsoft Defender for Cloud for threat detection and automated response.

5. Data Encryption and Segregation

- **Encryption in Transit:** All data transmission is encrypted using TLS 1.3.
- **Encryption at Rest:** Data is encrypted using AES-256. Database encryption utilises Transparent Data Encryption (TDE).
- **Data Isolation (Database-per-Tenant):** The Processor employs a "Database-per-Tenant" architecture. Each Customer is provisioned with a dedicated, logically separate Azure SQL Database, ensuring no cross-tenant data leakage.
- **Key Management:** Encryption keys are managed via Azure Key Vault using a vault-per-tenant (or similarly segregated) model.

6. Availability and Disaster Recovery

- **Resilience:** The Service utilises Azure Availability Zones and Region Pairing (e.g., UK South paired with UK West) to ensure redundancy against datacentre or regional failures.
- **Backups:**
  - Point-in-Time Restore (PITR) available for the last 14 days.

    - Long-term retention backups (Weekly, Monthly, Yearly) stored up to 7 years (extendable to 10).
- **Recovery Targets:** The Service is designed to meet defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) with a target availability of 99.8%.

7. Vulnerability Management

- **Vulnerability Scanning:** Automated Static Application Security Testing (SAST) and Software Composition Analysis (SCA) are integrated into the CI/CD pipeline.
- **Penetration Testing:** Independent, CREST-accredited (or equivalent) partners conduct formal penetration tests against the Service.
- **Patching:** The Processor aims to remediate Critical and High-risk vulnerabilities within 14 days of confirmation.

8. Supply Chain Security

- **Vendor Assessment:** All third-party sub-processors undergo a risk assessment. Key suppliers are monitored via the Risk Ledger platform.

Agreements: All sub-processors are bound by Data Processing Agreements (DPAs) ensuring GDPR alignment.

This Data Processing Agreement is entered into and becomes effective as of the date of signing by and between the Parties identified below.

IN WITNESS WHEREOF, the Parties have caused this Data Processing Agreement to be executed by their duly authorised representatives.

For and on behalf of the Controller	**For and on behalf of the Processor**
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date: