DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") forms part of the Master Services Agreement (the "**MSA**") between the customer named in the Order Form (the "**Customer**"), as data controller, and **Sala Daeng Company Limited** ("**SLD**"), as data processor. It applies to every Order Form that refers to it, and the Parties agree to it by signing that Order Form (clause 12.3). Terms defined in the MSA have the same meaning in this DPA. "Personal data", "data subject", "data controller", "data processor" and related terms have the meanings given in the Personal Data Protection Act B.E. 2562 (2019) (the "**PDPA**"). This DPA applies in the version stated in the Order Form. SLD publishes it at www.sala-daeng.com/agreements under its number and version.

1. Roles and Scope

1.1 In providing the Services, SLD processes the personal data in Customer Data on behalf of the Customer. The Customer is the data controller and SLD is the data processor of that personal data.

1.2 This DPA applies to all processing of personal data that SLD carries out on behalf of the Customer under any Contract Document. On the protection of personal data, this DPA prevails over the other Contract Documents, as MSA clauses 2 and 11 provide.

1.3 The Customer warrants that it has a lawful basis to collect, use and disclose the personal data it gives SLD to process, and that it has informed data subjects as the law requires.

1.4 **Minors.** Where the Order Form states that the data subjects include minors, such as students, the Customer warrants that it holds any consent the PDPA requires for the personal data of minors, including the consent of the person with parental responsibility where the law requires it, consistent with MSA clause 11.2.

1.5 **Permitted Affiliates.** The Customer gives instructions under this DPA for itself and on behalf of its Permitted Affiliates, and warrants that it is authorised to do so. Where a Permitted Affiliate is the data controller of personal data, SLD processes it on that Permitted Affiliate's behalf, and the Customer exercises the Permitted Affiliate's rights under this DPA.

1.6 **Sensitive data.** SLD does not process sensitive personal data under section 26 of the PDPA, such as health, religion or biometric data, unless the Order Form says so.

2. Details of Processing

2.1 Annex DPA-1 sets out the standard details of the processing for each setting in clause 2.2. The data processing section of the Order Form states which settings apply to the Customer and any additions, such as Permitted Affiliates, further data subjects or categories of personal data, minors, sensitive personal data and authentication. Those additions, and any details of the processing in a SOW, form part of Annex DPA-1 for that Customer.

2.2 SLD processes personal data in two settings:

(a) **Hosted Services.** SLD processes personal data on its cloud, using the sub-processors on the Sub-processor List (clause 6.1), as the Service Description describes.

(b) **Customer Environment.** For Customer-Hosted Software, Implementation Services, Maintenance and support, SLD's personnel access the Customer Environment remotely or on site. The personal data stays in the Customer's systems. SLD takes extracts out of the Customer Environment only for data migration, testing and support tickets, keeps them only in its systems on the Sub-processor List, and deletes them under clause 10.3.

3. SLD's Obligations as Data Processor

In line with section 40 of the PDPA, SLD will:

3.1 process personal data only on the Customer's documented instructions, being the Contract Documents and instructions given through the agreed channels, unless Thai law requires otherwise, in which case SLD will tell the Customer unless the law prohibits it;

3.2 tell the Customer promptly if it believes an instruction may breach the PDPA;

3.3 ensure that the persons it authorises to process personal data are bound by confidentiality duties and are appropriately trained in personal data protection;

3.4 maintain the security measures in clause 4 and review them periodically as risks change;

3.5 keep records of processing activities as the law requires, and make them available to the Office of the Personal Data Protection Committee on lawful request;

3.6 give the Customer reasonable help in responding to data subjects' requests to exercise their rights, in data protection impact assessments and in consultations with the Personal Data Protection Committee, at the Customer's reasonable cost where the effort is significant; and
3.7 not sell, disclose or use personal data for any purpose other than providing the Services under the MSA.

4. Security Measures

4.1 SLD maintains at least the following technical and organisational measures, as further described in the relevant Service Description:

Area	Measures
Infrastructure and encryption (Hosted Services)	Hosted on the cloud of an enterprise cloud provider certified to ISO/IEC 27001, as named on the Sub-processor List. Data in transit encrypted with TLS 1.2 or higher; data at rest encrypted with AES-256.
Access control and personnel	Role-based access control on the least-privilege principle; individual named user accounts; MFA or SSO as agreed in the SOW. Personnel are bound by confidentiality and access data only as needed to serve the Customer.
Access to the Customer Environment	Only the access methods and named accounts the Customer provides or approves, given only to personnel who need them, as MSA clause 12.3 provides. No local copies of personal data, except the extracts in clause 2.2(b).
Audit trail	For Hosted Services, an immutable audit trail of import, reading, checking, matching, editing, storage and approval, exportable as CSV. For Customer-Hosted Software, the software's own logs in the Customer Environment.
Segregation	Customer Data in Hosted Services is logically segregated from other customers' data, and only the documents and data the Customer brings into the service are processed.
Backup and restore	For Hosted Services, encrypted daily backups and documented, periodically tested restore procedures. Backups of the Customer Environment are the Customer's responsibility under MSA clause 4.2.
Development and vulnerabilities	Software development process certified to ISO/IEC 29110, regular security updates and application security testing by SLD's internal team. An external penetration test is arranged on request, at the Customer's cost.
Incident response	Documented incident response procedure, supporting notice to the Customer within 48 hours under clause 8 and notice to the Office of the Personal Data Protection Committee within 72 hours as the law requires.

4.2 SLD may update these measures, provided the overall level of protection is not reduced.

5. No Training of AI Models

5.1 SLD **will not use Customer Data, including personal data, to train, fine-tune or develop any artificial intelligence or foundation model**, whether its own or a third party's. It will configure and contract with the AI providers it uses so that data sent to them for processing is not used to train models, under those providers' enterprise data terms. Using users' review results and corrections and Customer Data to improve the checking rules, matching rules, templates, configurations and prompts used to serve the Customer is configuration under MSA clause 9.1, not training or fine-tuning a model.
5.2 SLD may use Usage Data in aggregated, de-identified form that contains no personal data, as MSA clause 9.5 allows.

6. Sub-processors

6.1 The Customer gives SLD general authorisation to use the sub-processors on SLD's sub-processor list, published at www.sala-daeng.com/trust/sub-processors (the "**Sub-processor List**"), for hosting, data storage, optical character

recognition (OCR), AI processing, remote access and support tools. The Sub-processor List states, for each sub-processor, its service, its processing locations and the SLD services it is used for.

6.2 SLD will (a) give the Customer at least 15 days' notice before adding or replacing a sub-processor, during which the Customer may object on reasonable data protection grounds. SLD gives this notice by posting the change on the Sub-processor List with the date it takes effect and by email to the Customer's contact for notices in the Order Form. For this clause, that email is sufficient notice without confirmation of receipt, notwithstanding MSA clause 21.1; (b) impose on each sub-processor data protection obligations no less protective than this DPA; and (c) remain fully responsible for each sub-processor's performance. Where a sub-processor stops or materially changes its service, or a change is urgently needed for security or continuity of the Services, SLD may make the change on shorter notice than in (a) and will notify the Customer as soon as practicable. The Customer's rights under clause 6.3 still apply.

6.3 If the Customer objects on reasonable grounds and the Parties cannot agree an alternative within 30 days, the Customer may terminate the affected Services by written notice and receive a pro-rata refund of the prepaid fees for the unused part of those Services.

6.4 Changing the AI model, AI provider or OCR provider within the Sub-processor List, including switching between services of the same sub-processor, is not an addition or replacement under clause 6.2.

6.5 The Customer's own hosting providers and other providers the Customer contracts for the Customer Environment are not SLD's sub-processors. The Customer is responsible for its agreements with them.

6.6 **The Sub-processor List.** Each version of the Sub-processor List shows the date it takes effect. SLD keeps past versions available and gives the Customer a PDF copy of the current version on request. Any person may sign up on the Sub-processor List page to receive the notices in clause 6.2 by email.

7. Transfers Outside Thailand

7.1 Hosted Services run in data centres of an enterprise cloud provider outside Thailand, and the OCR and AI providers process data outside Thailand, as named with their processing locations on the Sub-processor List. Hosted Services therefore involve transfers of personal data outside Thailand, as MSA clause 12.2 discloses and the Customer agrees. In the Customer Environment setting, personal data stays in the Customer's systems, except the extracts in clause 2.2(b) held in SLD's support tools on the Sub-processor List.

7.2 SLD will ensure that transfers of personal data outside Thailand comply with sections 28 and 29 of the PDPA and the subordinate legislation: transfers go to destinations with adequate protection standards as announced by the Personal Data Protection Committee, under appropriate safeguards (such as standard contractual clauses prescribed by the Committee, or binding corporate rules), or on another basis the law allows.

7.3 The Sub-processor List states each sub-processor's processing locations. Adding a location outside those listed for a sub-processor is a change under clause 6.2.

8. Personal Data Breach

8.1 SLD will notify the Customer **without undue delay, and in any case within 48 hours**, after becoming aware of a personal data breach affecting Customer Data in SLD's systems or caused by SLD's personnel. The notice will state, at once or in stages, the nature of the breach, the categories and approximate numbers of data and data subjects affected, the likely consequences, and the measures taken or proposed.

8.2 SLD will cooperate reasonably in the investigation, the remedy and any notice to the Office of the Personal Data Protection Committee or to data subjects. Those notices are decided and given by the Customer as data controller. For a breach in the Customer Environment not caused by SLD, SLD will give the Customer reasonable help on request.

9. Audit

9.1 SLD will give the Customer the information reasonably needed to show compliance with this DPA: the security assessment documents described in the relevant Service Description, the list of sub-processors and, for Hosted Services, the audit trail through the auditor role.

9.2 If the information in clause 9.1 is not sufficient, the Customer may audit SLD's compliance with this DPA no more than once in any 12 months, counted together with audits under MSA clause 12.6, unless a regulator orders an audit or a personal data breach has been confirmed. The Customer gives at least 20 Business Days' notice, the audit takes place during business hours, and the Customer bears its cost. The audit is subject to SLD's security and confidentiality policies and does not extend to other customers' data, SLD's cost data or the source code of SLD Software.

10. Return and Deletion

10.1 When the MSA or the relevant Order Form ends, SLD will return Customer Data and/or delete the remaining data and copies, as the Customer chooses, within the times and in the manner set out in MSA clause 17, unless Thai law requires the data to be kept, in which case clause 3 continues to apply to it. Backup copies are deleted in the normal rotation cycle and remain protected until deleted.

10.2 If the Customer instructs SLD to keep data under its own document retention policy (for example, tax documents for at least 5 years as the Revenue Department requires) while a Service continues, SLD will keep it as instructed, and this DPA applies throughout that period.

10.3 **Extracts.** SLD deletes extracts taken for data migration and testing within 30 days after the Go-Live of the phase they serve. Personal data in support tickets is kept with the ticket history while the Services continue and is deleted under clause 10.1 when they end. On request, SLD confirms deletion in writing.

11. Liability

Liability under this DPA is subject to the limitation of liability in MSA clause 15.

12. Term and Versions

12.1 This DPA takes effect when the MSA takes effect and continues for as long as SLD processes personal data on behalf of the Customer, including the return and deletion periods in clause 10.

12.2 SLD may issue a new version of this DPA for new Order Forms. A change to this DPA for an Order Form in effect must be in writing and signed by both Parties, except updates to the Sub-processor List under clause 6.2 and updates required by law, which SLD will notify to the Customer.

12.3 **Agreement and signature.** The Parties agree to this DPA by signing an Order Form that refers to it. It needs no separate signature. On request, SLD gives the Customer a copy signed by SLD.

12.4 **Languages.** SLD publishes this DPA in English and Thai, with the same content under the same version number. The language of the MSA the Customer signed governs.

Annex DPA-1 Details of Processing

This Annex sets out the standard details for each setting in clause 2.2. The data processing section of the Order Form states which settings apply and any additions, which form part of this Annex for that Customer.

Item	Hosted Services	Customer Environment
Subject matter	Providing the Hosted Services in the Order Form, such as BackOffice IQ	Implementation, maintenance and support of SAP Business One and SLD Software that run in the Customer Environment
Duration	The term of the MSA and the relevant Order Forms, including the return and deletion periods in clause 10	The same
Nature and purpose	Import and splitting of documents; OCR; classification; field-level data extraction; validation; checks of business partners, including queries to public databases of government agencies; matching with reference data from the Customer's accounting system; document storage; audit trail; data export; support	Configuration; data migration of master data and opening balances; testing; training; scheduled interface runs; support and troubleshooting; maintenance and upgrades
Data subjects	Personnel and representatives of the Customer's business partners; business partners who are individuals; the Customer's employees who use the service	The Customer's employees and system users; contacts of suppliers and customers; suppliers and customers who are individuals

Item	Hosted Services	Customer Environment
Categories of personal data	Names, positions, signatures and contact details (address, telephone, email); taxpayer identification numbers of individuals; bank account details shown on documents; user account data (name, email, role, activity logs)	Names, positions, signatures and contact details; taxpayer identification numbers of individuals; bank account details for payments and refunds; invoices, receipts and payment records; user account data (name, email, role, activity logs)
Sensitive personal data	None by intent. If it appears in a document by chance, it is processed only as part of the document image and is not extracted as data	None, unless the Order Form states otherwise. Fields holding sensitive data in a source system are not mapped into interfaces
Authentication	MFA or SSO as agreed in the SOW or the Order Form	As the Customer's systems provide, with the access methods in MSA clause 12.3

Annex DPA-2 Sub-processors

The approved sub-processors are those on the Sub-processor List (clause 6.1), at www.sala-daeng.com/trust/sub-processors. The Customer's own hosting provider and other providers it contracts for the Customer Environment are not SLD's sub-processors (clause 6.5).