DATA PROCESSING AGREEMENT

Idaraa Cloud Platform

Processor	Clarisolv LLC (Delaware file no. 10206059)
Customer	The customer identified in the applicable Order Form or Main Agreement
Effective date	The effective date of the Main Agreement
Version	1.0 | 21 August 2026

Definitions and scope

This DPA applies wherever Clarisolv processes personal data on Customer's behalf in providing Idaraa. "Applicable Data Protection Law" means the EU GDPR, the UK GDPR, and any other privacy, data-protection or cybersecurity law that applies to that processing; "Controller," "Processor," "Data Subject," "Personal Data," "Processing," "Supervisory Authority" and "Personal Data Breach" carry the meanings given by that law. For Customer Personal Data, Customer is the Controller and Clarisolv is the Processor, except where Customer itself acts as a processor for another controller, in which case Clarisolv acts as Customer's subprocessor. Customer determines the purposes and means of processing and is responsible for its own instructions, notices, lawful bases, consents, data accuracy, and data-subject rights, and must not instruct Clarisolv to process personal data unlawfully. If there is ever a conflict specifically about the processing of Customer Personal Data, this DPA and any incorporated transfer clauses take precedence over the Main Agreement; otherwise the Main Agreement governs as usual.

Processing instructions

Clarisolv processes Customer Personal Data only on Customer's documented instructions — the Main Agreement itself, Customer's configuration and use of the Service, accepted support requests, and other written instructions — unless a law that applies to Clarisolv requires otherwise, in which case Clarisolv will tell Customer about that legal requirement first unless the law prohibits it. If, in Clarisolv's reasonable opinion, an instruction would infringe Applicable Data Protection Law, Clarisolv will say so promptly and may pause the affected processing until the parties agree a lawful instruction, without excusing Customer from its payment obligations for unaffected parts of the Service. The subject matter, purpose, duration, and categories of data and data subjects involved are set out in Schedule 1.

Confidentiality and personnel

Everyone Clarisolv authorises to process Customer Personal Data is bound by a duty of confidentiality — contractual or statutory — and only has access to what their role requires, with privacy and security guidance appropriate to that role.

Security

Clarisolv maintains technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access, calibrated to the state of the art, implementation cost, and the nature and risk of the processing involved. The measures currently in place are described in Schedule 2; Clarisolv may update them over time, but never in a way that materially reduces the overall level of protection. Customer is responsible for its own side of this — securely configuring its account, assigning roles on a least-privilege basis, protecting its own credentials, enabling stronger authentication where available, promptly disabling former users, and otherwise using the Service consistently with the Main Agreement and Clarisolv's documented guidance.

Personal data breaches

If Clarisolv becomes aware of a confirmed Personal Data Breach affecting Customer Personal Data, it will notify Customer without undue delay, in phases if needed as facts become available — covering, to the extent reasonably known, what happened, the likely consequences, what's being done about it, and a contact point for follow-up. Clarisolv will take reasonable steps to contain, investigate, and remediate the breach and will reasonably support Customer's own legally required notifications, but notifying Customer is not an admission of fault, and it remains Customer's decision — not Clarisolv's — whether to notify a supervisory authority, data subjects, or anyone else, unless a law assigns that duty to Clarisolv directly.

Subprocessors

Customer gives Clarisolv general written authorisation to engage the subprocessors listed in Schedule 3, and any others in accordance with this section. Clarisolv will normally give Customer at least 15 days' notice — by email, in-product notice, or an updated subprocessor page — before an intended new or replacement subprocessor materially processes Customer Personal Data. Customer may object on reasonable, documented data-protection grounds during that notice period; if the parties can't reach a commercially reasonable resolution, Clarisolv may simply not use that subprocessor for Customer, or Customer may terminate only the affected part of the Service and receive a pro-rata refund of prepaid fees for the terminated post-effective-date period. Not objecting within the notice period counts as approval. Clarisolv imposes written data-protection obligations on every subprocessor that are materially equivalent to its own obligations under this DPA, and remains responsible to Customer for how its subprocessors perform them.

Data subject requests

Clarisolv provides reasonable technical and organisational assistance to help Customer respond to data subjects exercising their rights under Applicable Data Protection Law. If a request comes to Clarisolv directly about Customer Personal Data, Clarisolv will — unless legally prohibited — redirect the requester to Customer or forward the request, rather than responding to it substantively itself, unless Customer instructs otherwise or the law requires a direct response. If a request needs material custom work beyond the Service's standard functionality, the parties agree the scope, timing, and any reasonable charges in advance, except where a charge would itself be unlawful.

Compliance assistance and audits

Taking into account the nature of the processing and what information is available to it, Clarisolv provides reasonable assistance with Customer's own security-of-processing, breach-notification, data-protection-impact-assessment, and supervisory-authority-consultation obligations, to the extent they relate to Customer's use of the Service — and will share information reasonably necessary to demonstrate Clarisolv's own compliance, which Customer may use only for compliance, audit, and risk-management purposes and must protect as confidential. Customer may audit Clarisolv's compliance with this DPA once in any 12-month period (or more often if justified by a breach, a supervisory-authority request, or reasonable evidence of material non-compliance) — ordinarily satisfied through current security documentation, questionnaires, available independent-assessment

summaries, and remote interviews first, with an on-site inspection by an independent, non-competitor auditor available if that's genuinely not enough. On-site audits need at least 20 business days' written notice, happen during normal business hours, must minimise disruption and stay within confidentiality obligations, and Customer bears the cost unless the audit turns up a material breach by Clarisolv.

Return and deletion

During the term, Customer can export its Personal Data through the Service's own functions, or request reasonable export assistance under the Main Agreement. When the relevant part of the Service ends, Clarisolv will return or delete Customer Personal Data as Customer chooses, after a reasonable transition period, unless the law requires it to be retained — if Customer doesn't choose within 30 days, Clarisolv deletes it under its standard secure-deletion process. Data that ends up in backups or disaster-recovery copies may be kept until it's naturally overwritten or deleted in the ordinary backup cycle, as long as it stays isolated from routine use and is only ever restored for disaster recovery, legal compliance, or security purposes — any restored copy is still subject to the original deletion instruction. Clarisolv may also keep minimal records needed to demonstrate contract performance, resolve disputes, prevent fraud, enforce its rights, or comply with the law, acting as an independent controller for that narrow purpose.

Government and third-party demands

Unless prohibited by law, Clarisolv will tell Customer about a legally binding demand for Customer Personal Data before disclosing anything — checking the demand's validity, disclosing only what's actually legally required, and reasonably supporting Customer's own lawful efforts to challenge or narrow it, at Customer's cost.

International transfers

Customer authorises Clarisolv and its subprocessors to process Customer Personal Data in the locations described in Schedule 3, subject to this DPA and Applicable Data Protection Law; Customer stays responsible for identifying any restricted transfer that its own configuration or instructions create. Where EU GDPR applies to a transfer to a country the European Commission hasn't recognised as adequate, and no other lawful transfer mechanism applies, the parties incorporate the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914) as completed in Schedule 4, and won't modify them except as those clauses themselves permit. Where UK GDPR applies and no other mechanism applies, the parties use the then-current UK International Data Transfer Addendum to those clauses, completed consistently with Schedule 4. Both parties will reasonably cooperate on any required transfer risk assessment and supplementary safeguards, and if a transfer mechanism ever becomes invalid, will work in good faith toward a valid alternative — suspending or terminating only the affected processing if none is reasonably available.

Sensitive data and prohibited use

Customer must not submit government ID numbers, payment-card authentication data, biometric templates, criminal records, precise geolocation, or other highly sensitive data unless the Service expressly supports it, it's necessary for the agreed purpose, and it's lawful under Applicable Data

Protection Law. Where Customer enables pharmacy or similar workflows, it may instruct processing of prescription indicators, medicine or order details, or other information that could reveal health information — Customer is responsible for having a lawful basis, limiting access, giving any required notices, and avoiding unnecessary health data, while Clarisolv applies this DPA's safeguards without itself determining whether Customer's use is legally permitted. The Service isn't intended for direct use by children unless expressly agreed in writing, and Customer must not knowingly use it to collect children's personal data without the legally required notices, consents, and protections in place.

Liability

Each party's liability under this DPA is subject to the same exclusions, limitations and allocation of liability set out in the Main Agreement, except where Applicable Data Protection Law or an incorporated transfer clause prohibits that. Nothing in this DPA limits a data subject's own rights or a supervisory authority's own powers under Applicable Data Protection Law.

Term and termination

This DPA takes effect on the Main Agreement's effective date and remains in force for as long as Clarisolv processes Customer Personal Data. Provisions that are meant by their nature to survive — confidentiality, deletion, audit evidence, international transfers, and liability — continue to apply after termination for as long as any relevant Customer Personal Data remains in Clarisolv's possession or control.

Notices

Notices under this DPA are sent in accordance with the Main Agreement. Privacy and security notices to Clarisolv can also be sent to info@idaraa.com. Customer should keep a current administrative and privacy contact on file in its account or Order Form.

Governing law

This DPA is governed by whichever law and dispute forum the Main Agreement specifies. If the Main Agreement is silent, this DPA is governed by the laws of the State of Delaware, without regard to conflict-of-laws rules, and the parties submit to the state and federal courts located in Delaware — in each case subject to mandatory Applicable Data Protection Law and to the governing-law and forum provisions of any incorporated transfer clauses.

Schedule 1 — Details of processing

Subject matter: provision, administration, security, support and improvement of the Idaraa cloud platform for Customer's business operations. Duration: the term of the Main Agreement, plus any limited transition, backup or legally required retention period described in this DPA. Nature and purpose: collection, recording, organisation, structuring, storage, retrieval, consultation, use, transmission within authorised integrations, reporting, export, restriction, deletion and other processing necessary to provide the Service on Customer's instructions. Frequency: continuous, or as initiated by Customer and its authorised users during the term. Categories of data subjects:

Customer's authorised users and personnel; Customer's customers and prospective customers; loyalty programme members; suppliers and their representatives; delivery recipients; and other individuals whose data Customer chooses to enter into the Service. Categories of personal data: names; business and personal contact details; account and role information; store, branch and employment information; customer identifiers; order, invoice, return, payment-status and transaction history (excluding full card credentials, which Idaraa does not store); loyalty points and preferences; delivery details; product and inventory interactions; support communications; device, login, audit and security logs; imported spreadsheet data; and data contained in Customer-configured fields. Sensitive or special-category data: not required for standard retail use — in pharmacy or similar deployments, prescription indicators, medicine or order details, or Customer-submitted content may reveal health information, and this only happens if Customer enables and instructs it, with Customer responsible for its legal basis and for minimising what it submits. Processing operations: hosting and tenant administration; authentication and access control; transaction and inventory processing; reporting; bulk catalogue import; support and troubleshooting; backup and disaster recovery; email delivery; security monitoring; and operation of Customer-authorised integrations.

Schedule 2 — Technical and organisational measures

The measures below describe the current control framework for the Service. They are risk-based and may evolve, provided the overall level of protection is never materially reduced. Access control: tenant and branch separation, role-based permissions, least-privilege administration, individual user accounts, temporary passwords requiring reset, and controlled provisioning/deprovisioning. Authentication: rate-limited sign-in, secure credential handling, and time-based one-time-password multi-factor authentication where enabled or available for the account. Encryption: HTTPS/TLS for data in transit and Microsoft Azure platform encryption for supported data at rest, with cryptographic keys and platform controls managed according to the applicable hosting configuration. Hosting and resilience: production hosting in Microsoft Azure UAE North, with platform resilience, monitoring and backup capabilities configured for the Service. Logging and traceability: application and administrative audit trails for relevant actions, security logging, and reasonable review of suspicious access or operational events. Secure operations: controlled deployment and change practices, separation of production access from ordinary user access, and vulnerability and dependency management proportionate to risk. Data minimisation: service fields and access are limited to the functions Customer configures; full payment-card credentials are not stored by Idaraa, and payment providers, where enabled, process card credentials under their own terms. Confidentiality: personnel and contractors with authorised access are bound by confidentiality obligations and receive access according to role and operational need. Availability and recovery: backups and recovery procedures proportionate to the Service, with restoration limited to authorised continuity, security and legal purposes. Customer controls: customer-controlled user roles, branch access, password reset, data export and configuration features, plus optional enhanced authentication where available. Incident response: processes to identify, contain, investigate, remediate and communicate confirmed incidents affecting Customer Personal Data. Review: periodic review of these measures in light of material service changes, threats and legal requirements.

Schedule 3 — Approved subprocessors and recipients

Customer generally authorises the following providers; Clarisolv completes each provider's precise legal entity and location before first signature and maintains the current list after that. Microsoft Ireland Operations Limited — application, database, storage, backup and outbound email infrastructure; hosted in UAE North, with other locations only as documented; subprocessor. Hostinger International Ltd. — hosting for the info@idaraa.com support mailbox; located as configured in the applicable hosting account; subprocessor only to the extent Customer Personal Data enters that mailbox. Customer-selected payment provider — payment authorisation and settlement when enabled; location as selected by Customer; not enabled by default, and generally an independent recipient under its own terms. Customer-selected delivery or order integration — order transmission, fulfilment or delivery when enabled; location as selected by Customer; may be an independent recipient, classified before activation. Subprocessor-change notices go to the current administrative or privacy contact Customer maintains; objections follow the process described above.

Schedule 4 — Restricted transfer terms

For EU transfers: where the EU Standard Contractual Clauses apply, Module Two (controller-to-processor) applies where Customer is a controller, and Module Three (processor-to-processor) applies where both relationships occur, with the relevant module applying to the relevant processing. The Clause 7 docking clause applies; general written authorisation applies for Clause 9 subprocessor changes, using the notice period described above; the optional independent dispute-resolution language under Clause 11 does not apply; the governing law under Clause 17 is that of the EU member state named in the applicable Order Form, or Irish law if none is named, with that member state's courts having jurisdiction under Clause 18. The data exporter is Customer and the data importer is Clarisolv LLC, with identities, addresses and contacts as stated in the Main Agreement and applicable Order Form; the transfer details, processing description, technical and organisational measures, and subprocessor list are completed by Schedules 1, 2 and 3 respectively, and the EU clauses are deemed signed on execution of this DPA — if they ever conflict with this DPA, the EU clauses prevail for the restricted transfer they cover. For UK transfers: where a UK restricted transfer needs contractual safeguards, the parties incorporate the then-current UK International Data Transfer Addendum issued by the UK Information Commissioner's Office (or another mechanism validly agreed in writing), using the same parties and transfer details as above; if the Information Commissioner's Office issues a revised addendum, neither party may terminate solely because of that, and the parties will reasonably cooperate to implement the revised terms instead. For other jurisdictions: where a restricted transfer is governed by another jurisdiction's law, the parties will incorporate or execute whatever mandatory standard clauses or approved transfer mechanism the Service reasonably requires, completed using the information in this DPA wherever that's permitted.

Schedule 5 — Customer-specific details and signatures

Each customer's specific details — legal name, registered address, the Main Agreement or Order Form it's tied to, its privacy contact, any special processing instructions or approved sensitive data beyond what's described above, and (where the EU Standard Contractual Clauses apply) the governing law and courts selected for them — are completed and signed by both parties as part of

executing this DPA with that customer's account, rather than published here. Contact info@idaraa.com to execute a customer-specific DPA for your business.

Clarisolv LLC — Idaraa Cloud Platform — Data Processing Agreement, Version 1.0. This is a general reference copy; a customer-specific copy including Schedule 5 is completed and signed as part of onboarding.