LEGAL / VERSION 1.1

Data Processing Addendum.

Article 28 terms for customer-controlled Flow responses, durable records and future signature artifacts.

LAST UPDATED	EFFECTIVE	SCOPE
15 July 2026	On acceptance	Business customers

This Data Processing Addendum (DPA) forms part of the ProseID Terms of Service or another agreement that references it (the Agreement). It applies when ProseID processes Customer Personal Data on the Customer's behalf.

The Customer is the controller and ProseID is the processor for Customer Personal Data. ProseID remains an independent controller for its own account administration, billing, security, abuse-prevention and legal-compliance processing described in the Privacy Policy.

PROCESSOR CONTACT

ProseID
Edingekroken 12, 163 63 Spånga, Stockholm, Sweden
hello@alentra.app

CONTENTS

Agreement structure

01 Definitions and interpretation

Applicable Data Protection Law means the GDPR, the Swedish Data Protection Act and any other data-protection law that applies to the processing. Customer means the business or professional user that accepts the Agreement. Customer Personal Data means personal data contained in data submitted to, collected through or generated for the Customer's use of the service. ProseID means the service provider identified as the operator in the Terms of Service.

Controller, processor, personal data, processing, data subject, personal data breach and supervisory authority have the meanings given by Applicable Data Protection Law. Subprocessor means a processor engaged by ProseID to process Customer Personal Data.

02 Scope and order of precedence

This DPA governs ProseID's processing of Customer Personal Data as a processor. If this DPA conflicts with the Agreement on data-protection matters, this DPA controls. The Agreement otherwise remains unchanged.

The details of the processing required by Article 28(3) GDPR are in Annex I. The technical and organisational measures are in Annex II. The current Subprocessors are in Annex III and on the maintained Sub-processors page.

03 Documented instructions

ProseID will process Customer Personal Data only on the Customer's documented instructions, including those expressed through the Agreement, this DPA, the Customer's schemas, Flows, delivery settings, API requests and support requests, unless Union or Member State law requires otherwise. If legally permitted, ProseID will tell the Customer before carrying out processing required by law.

ProseID will promptly inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law and may suspend the affected processing while the parties resolve the issue. ProseID does not determine which personal data the Customer chooses to request through a schema.

04 Customer responsibilities

The Customer determines the purposes and essential means of processing Customer Personal Data. The Customer is responsible for the lawfulness, fairness and transparency of its collection; the accuracy of its instructions; its notices and lawful bases; responding to data-subject requests; and selecting and periodically reviewing appropriate retention periods.

The Customer will not instruct ProseID to process special-category or criminal-offence data unless the Customer has identified an applicable legal condition and implemented any additional safeguards required by law.

05 Confidentiality and personnel

ProseID will ensure that personnel authorised to process Customer Personal Data are bound by confidentiality obligations, receive access only where necessary for their duties and process the data only in accordance with the Customer's instructions and this DPA.

06 Security

Taking into account the state of the art, implementation costs, the nature, scope, context and purposes of processing, and the risks to individuals, ProseID will maintain appropriate technical and organisational measures under Article 32 GDPR. The current measures are described in Annex II.

Encryption protects confidentiality but does not make data anonymous where ProseID can decrypt it to provide the service. Production submission and signature payloads are encrypted at the application layer with Google Cloud KMS, bound to the owning organisation and decrypted server-side only after authorisation.

07 Subprocessors

The Customer gives ProseID general written authorisation to engage the Subprocessors listed in Annex III. ProseID will impose data-protection obligations on each Subprocessor that are no less protective, in substance, than the obligations applicable to that Subprocessor's processing under this DPA. ProseID remains responsible for each Subprocessor's performance to the extent required by Applicable Data Protection Law.

ProseID will give notice by email, in-product notice or an update to the maintained Sub-processors page before a new or replacement Subprocessor begins processing Customer Personal Data, except where an urgent security or legal need makes advance notice impracticable. The Customer may object on reasonable data-protection grounds within 15 days. The parties will work in good faith on a reasonable alternative; if none is available, either party may terminate the affected service without penalty.

08 International transfers

ProseID will not transfer Customer Personal Data outside the EEA except in accordance with Applicable Data Protection Law. Where a transfer is not covered by an adequacy decision, ProseID will use an approved transfer mechanism, including the European Commission's Standard Contractual Clauses where appropriate, and implement supplementary safeguards where the transfer assessment requires them.

09 Assistance and data-subject rights

Taking into account the nature of the processing and information available to it, ProseID will reasonably assist the Customer with data-subject requests and with the Customer's obligations concerning security, breach notification, data-protection impact assessments and prior consultation with a supervisory authority.

If ProseID receives a request directly from a person concerning Customer Personal Data, it will direct the person to the Customer and will not respond substantively unless instructed by the Customer or required by law.

10 Personal data breaches

ProseID will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. As information becomes available, the notice will describe the nature of the breach, affected data and data subjects, likely consequences, mitigation taken or proposed and a contact point. ProseID will take reasonable steps to contain, investigate and remediate the breach and will cooperate with the Customer's legally required notifications.

11 Return, deletion and durable records

Durable verification evidence is a core purpose of the service. By creating completed records, the Customer instructs ProseID to retain their encrypted submission payloads, validation records, proofs and any signature artifacts while the Agreement is active and, unless a deletion instruction is actioned, after account closure so that the Customer's records remain verifiable. The Customer is responsible for ensuring that this instruction has a lawful basis and remains necessary for its stated retention period.

At any time, and on termination, a Customer organisation owner or administrator may submit one or more owned completed-record identifiers through the service as a deletion instruction. After authorised ProseID staff validate and action the instruction, access through the Customer workspace, API, proof and receipt routes ends immediately. The affected records then remain in a restricted administrative recovery state for 30 days so that an accidental instruction can be reversed. At the end of that period, ProseID permanently deletes the submission payload, validation proof, signature artifacts, delivery copies and completed Flow link.

Before actioning an instruction, ProseID may defer deletion to the extent Union or Member State law requires storage or limited retention is necessary for the establishment, exercise or defence of legal claims. Data retained for such an exception will be restricted, protected and deleted when the exception ends. After permanent deletion, ProseID retains only a minimal payload-free administrative audit and anti-recreation record, together with financial or other records it must retain as an independent controller. The Customer acknowledges that deleting a signed payload prevents later verification of the signature against its original contents.

Customer Personal Data in backups will be put beyond ordinary use and removed through the normal backup rotation, unless law requires longer retention. ProseID will not use retained Customer Personal Data for advertising or unrelated product purposes.

12 Information and audits

ProseID will make available information reasonably necessary to demonstrate compliance with Article 28 GDPR. No more than once in any 12-month period, unless required by a supervisory authority or following a relevant breach, the Customer may request a reasonable audit by an independent auditor bound by confidentiality.

Audits must be scheduled on reasonable notice, minimise disruption, avoid access to other customers' data and not compromise security. The Customer bears its audit costs unless the audit identifies a material breach of this DPA by ProseID. ProseID may first satisfy an audit request with current security documentation, questionnaires or independent reports where these reasonably address the request.

13 Government requests

Unless legally prohibited, ProseID will notify the Customer of a binding government request for Customer Personal Data before disclosure. ProseID will review the request for validity, challenge unlawful or disproportionate requests where reasonable and disclose only the data legally required.

14 Term, changes and liability

This DPA takes effect when the Customer accepts the Agreement or first submits Customer Personal Data to the service and continues while ProseID processes Customer Personal Data. ProseID may update this DPA to reflect law, regulatory guidance or service changes, but will not materially reduce the protection of Customer Personal Data without reasonable notice.

The liability provisions and governing law in the Agreement apply to this DPA. If the parties execute a separately signed data-processing agreement, that signed agreement controls to the extent of any conflict.

ANNEX I

Details of processing

Subject matter	Hosting schema-defined Flows; receiving, validating, encrypting, storing and delivering submissions; producing verification records and proofs; and relaying signature requests and results when signing is enabled.
Nature and purpose	Collection, transmission, organisation, validation, encryption, storage, authorised decryption, retrieval, delivery, export, restriction and deletion as necessary to provide the service under the Customer's instructions.
Duration	For the Agreement term and the customer-directed evidence-retention period described in section 11. After a validated deletion instruction is actioned, access ends immediately, followed by a 30-day restricted recovery period and permanent deletion, subject to limited legal retention.
Frequency	Continuous or event-driven, depending on the Customer's use of Flows, APIs, delivery channels and account features.
Data subjects	People who complete Customer Flows; recipients of Flow links or receipts; Customer personnel, users and invited organisation members; and people represented in Customer-provided records.
Personal data	Schema-defined responses; names, contact and delivery details where requested; typed or provider-returned signature data; record and device metadata; customer identifiers; validation outcomes; schema and Flow references; delivery records; and support instructions.
Sensitive data	The service does not require special-category or criminal-offence data by default. Such data may be processed only where the Customer deliberately configures a schema to collect it and has a valid legal condition and appropriate safeguards.

ANNEX II

Technical and organisational measures

01	Encryption in transit using TLS and provider-managed encryption at rest for hosted infrastructure.
02	Application-layer encryption of production submission and signature payloads using Google Cloud KMS. Additional authenticated data binds ciphertext to the owning organisation, and cross-organisation decryption fails closed.
03	Server-side decryption only after authentication and active organisation-membership or API-key authorisation checks. Sensitive payloads are not directly readable from the browser database client.
04	Tenant isolation through organisation-scoped access checks, restrictive Firestore rules and server-mediated public submission writes with authoritative revalidation.
05	Role-limited administrative access, confidentiality obligations and access granted according to operational need.
06	Tamper-evident record proofs containing cryptographic response and output digests, immutable published schema versions and recorded signing-provider references when applicable.
07	Cloud audit logging for KMS operations and operational logging for security, delivery and administrative events, subject to access controls.
08	Documented incident handling, dependency and code review practices, automated tests and deployment checks proportionate to the service's risk.
09	Managed hosting, database resilience and backup processes supplied by the infrastructure providers, with restoration and continuity procedures appropriate to the service.
10	Data minimisation controls including request-size limits, schema-defined fields, purpose-limited delivery and separation of account, billing, verification and completion records.

ANNEX III

Authorised Subprocessors

Google (Firebase and Google Cloud)	Authentication, Firestore database, Cloud Functions, Storage, Cloud KMS and consent-gated analytics. Processing locations may include the EEA and United States.
Railway	Hosting the ProseID web application and API. Processing locations may include the EEA and United States.
Zoho (ZeptoMail)	Transactional delivery of receipts, PDFs, Flow links and service messages through the provider's EU data centre when the Customer configures or requests email delivery.

Stripe handles customer payment and card data for billing and is described separately in the Privacy Policy and Sub-processors page; it does not receive hosted-Flow submission payloads under this DPA. UIP is not yet active. Before UIP processes Customer Personal Data, ProseID will add it to the maintained list and provide notice under section 7.

END OF ADDENDUM

Questions: hello@alentra.app