

Data Processing Agreement

Ongo Agility / GDPR processor and data-governance terms

Version 2026-27 / Updated 8 September 2026

Version 2026-27 | Updated 8 September 2026

Draft for legal review. Prepared for Ongo Systems B.V. This document should be reviewed by Dutch legal counsel before first external use and read together with the Master Service Agreement, applicable Order Form and, where applicable, the Acceptable Use Policy, Service Level Agreement, Security Schedule and regulatory addenda.

This Data Processing Agreement (the "DPA") forms part of the Agreement between Ongo Systems B.V. ("Ongo") and the Customer identified in the applicable Order Form ("Customer"). It applies where Ongo processes Personal Data on behalf of Customer in connection with the Services. Capitalised terms not defined in this DPA have the meanings given in the Master Service Agreement ("MSA").

The Parties intend this DPA to satisfy Article 28 of Regulation (EU) 2016/679 (the "GDPR") and equivalent processor-contract requirements under Applicable Data Protection Law. The DPA allocates obligations according to each Party's actual legal role and does not transfer to either Party obligations imposed directly on the other by law.

1. SCOPE, ROLES AND DEFINITIONS

1.1 For Personal Data processed by Ongo on Customer's behalf in providing the Services, Customer acts as controller and Ongo acts as processor, unless the applicable Order Form expressly identifies another lawful role allocation. Where Customer acts as a processor for another controller, Ongo acts as Customer's subprocessor for that processing and Customer represents that it is authorised to appoint Ongo and issue the relevant instructions.

1.2 Each Party remains independently responsible for processing for which it determines the purposes and essential means and therefore acts as controller. This DPA does not govern Ongo's limited independent-controller processing of its own business contact, billing, corporate-security, legal-compliance or relationship-management data, to the extent Ongo determines the purposes and means of that processing and it does not consist of Customer content processed on Customer's behalf.

1.3 The subject matter, duration, nature and purpose of processing, categories of Personal Data and categories of Data Subjects are set out in Annex 1 and may be further specified in the applicable Order Form. Customer is responsible for ensuring that those particulars remain materially accurate for the Customer-controlled use of the Services.

1.4 "Applicable Data Protection Law" means the GDPR, the Dutch GDPR Implementation Act (Uitvoeringswet Algemene verordening gegevensbescherming) where applicable, and other binding data-protection or privacy law applicable to the relevant processing. "Personal Data", "Processing", "Controller",

"Processor", "Data Subject", "Personal Data Breach" and equivalent terms have the meanings given in Applicable Data Protection Law. "Subprocessor" means another processor engaged by Ongo to process Personal Data on Customer's behalf.

2. DOCUMENTED INSTRUCTIONS AND CUSTOMER RESPONSIBILITIES

2.1 Ongo shall process Personal Data only on documented instructions from Customer, including with regard to transfers to a third country or international organisation, unless Ongo is required to process the Personal Data by Union or Member State law to which Ongo is subject. Where legally permitted, Ongo will inform Customer of that legal requirement before the processing.

2.2 Customer's documented instructions consist of the Agreement, the applicable Order Form, Customer's authorised configuration and use of the Services, and other written instructions accepted by Ongo. Instructions

that require materially different processing, architecture, security controls, integrations or Professional Services may be subject to change control, additional Fees or a separate written agreement.

2.3 Customer is responsible for the lawfulness of its instructions and for establishing the legal bases, notices, consents, permissions and other conditions required for Customer to collect, use, disclose and instruct Ongo to process the Personal Data. Customer shall not instruct Ongo to process Personal Data in a manner that violates Applicable Data Protection Law or the Agreement.

2.4 Ongo shall inform Customer without undue delay if, in Ongo's reasonable opinion, a Customer instruction infringes Applicable Data Protection Law. Ongo may suspend the affected processing to the extent reasonably necessary while the Parties address the issue. Ongo is not required to perform an instruction that would itself be unlawful.

3. CONFIDENTIALITY AND AUTHORISED PERSONNEL

3.1 Ongo shall ensure that persons authorised to process Personal Data are subject to contractual, statutory or professional confidentiality obligations appropriate to the information and receive access only to the extent reasonably necessary for their functions.

3.2 Ongo shall maintain access-governance processes designed to grant, review, adjust and revoke personnel access in accordance with role and operational need. Customer remains responsible for access granted through Customer-controlled accounts, roles, endpoints, credentials and integrations.

4. SECURITY OF PROCESSING

4.1 Taking into account the state of the art, implementation costs, and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, Ongo shall implement and maintain appropriate technical and organisational measures designed to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

4.2 The baseline technical and organisational measures are described in Annex 2. Measures may be updated as technology, threats and the Services evolve, provided that Ongo does not materially reduce the overall level of security of the contracted processing during an active Order Term without a lawful reason or an agreed alternative.

4.3 Security is shared across the agreed service boundary. Customer shall secure Customer Systems, endpoints, identity providers, credentials, user administration and Customer-controlled integrations; configure permissions according to least privilege; and implement Customer-side measures reasonably appropriate to the use case and risk.

4.4 Where the agreed deployment is Customer-hosted, on-premises or otherwise places specified infrastructure or security controls under Customer's control, the Order Form or Security Schedule may allocate the corresponding responsibilities to Customer. Ongo is not responsible for a control that the Agreement expressly places outside Ongo's managed service boundary.

5. PERSONAL DATA BREACHES

5.1 Ongo shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA. The notification may be made in phases where information is not available at the same time.

5.2 To the extent reasonably available to Ongo, the notification or subsequent updates will include information concerning:

- (a)** the nature of the Personal Data Breach and, where possible, the categories and approximate number of affected Data Subjects and records;
- (b)** the known or reasonably anticipated consequences of the Personal Data Breach;
- (c)** the measures taken or proposed by Ongo to contain, investigate, remediate or mitigate the Personal Data Breach; and
- (d)** a contact point through which Customer can obtain relevant follow-up information.

5.3 Ongo shall provide reasonable cooperation and information available to it to assist Customer with Customer's obligations under Articles 33 and 34 GDPR or equivalent Applicable Data Protection Law. Customer remains responsible for determining whether and how to notify a supervisory authority, Data Subjects or other third parties, unless Applicable Data Protection Law imposes a direct notification obligation on Ongo.

5.4 A Personal Data Breach notification, investigation, mitigation step or related cooperation does not constitute an admission of fault, breach or liability by Ongo.

6. SUBPROCESSORS

6.1 Customer gives Ongo general written authorisation to engage Subprocessors necessary to provide, host, secure, support or operate the Services, subject to this Section 6.

6.2 Ongo shall maintain and make available current information sufficient to identify the Subprocessors in the processing chain relevant to Customer Personal Data, including, to the extent applicable and reasonably available, the Subprocessor's legal name, service or processing purpose, principal processing location and applicable international-transfer basis. The operational register may be maintained online or in a separate schedule referenced in Annex 3.

6.3 Where reasonably practicable, Ongo will give Customer at least thirty (30) days' prior notice before a new direct Subprocessor begins processing Customer Personal Data, or before a material replacement, so that Customer has an opportunity to object on reasonable and documented data-protection grounds. A shorter notice period may be used where an urgent security, legal, continuity or third-party dependency requires faster action; Ongo will provide notice as soon as reasonably practicable in that case.

6.4 Ongo shall carry out proportionate due diligence on direct Subprocessors and impose written data-protection obligations that are materially no less protective than the obligations applicable to Ongo under this DPA to the extent relevant to the Subprocessor's processing. Ongo remains responsible for the performance of its direct Subprocessors as required by Article 28(4) GDPR, subject to the limitations of liability in the Agreement.

6.5 If Customer raises a valid objection under Section 6.3, the Parties will work in good faith to address it. Ongo may avoid or replace the affected Subprocessor, offer a commercially reasonable alternative configuration, or take another appropriate measure. If no commercially reasonable solution is available and the objection concerns a material data-protection risk, Customer may terminate only the affected Service before the new Subprocessor begins the disputed processing, and Ongo shall refund prepaid recurring Fees for the terminated portion covering the period after termination.

6.6 Customer acknowledges that its controller accountability obligations may require it to evaluate whether the processing chain provides sufficient guarantees. Ongo will provide information reasonably available to it for that assessment, subject to confidentiality, security, proportionality and protection of third-party rights. Ongo is not required to disclose full unredacted Subprocessor contracts where equivalent compliance evidence reasonably addresses the request, unless Applicable Data Protection Law or a competent authority requires otherwise.

7. INTERNATIONAL TRANSFERS

7.1 Ongo shall not transfer Personal Data to a country or international organisation outside the European Economic Area ("EEA"), or permit an onward transfer requiring a Chapter V GDPR mechanism, unless a lawful transfer basis and any required safeguards are in place.

7.2 A lawful transfer basis may include an applicable European Commission adequacy decision, including participation by an eligible recipient in an adequacy framework recognised by the European Commission, or appropriate safeguards under Article 46 GDPR such as the then-current European Commission Standard Contractual Clauses ("SCCs").

7.3 Where SCCs are required for a transfer for which Ongo is the data exporter, Ongo shall enter into the applicable SCC module with the relevant data importer and complete the required annex information. Where required by Applicable Data Protection Law, Ongo will assess the transfer circumstances and implement supplementary contractual, technical or organisational measures appropriate to the transfer risk.

7.4 Ongo shall make relevant transfer documentation reasonably available to Customer where necessary for Customer to assess compliance with Articles 28 and 44 to 49 GDPR, subject to redaction of information not relevant to Customer, confidentiality, security and third-party rights. Customer remains responsible for its own assessment of transfers and sufficient guarantees to the extent required by law.

7.5 If a relied-upon transfer mechanism is invalidated, withdrawn or becomes unavailable, the Parties will cooperate in good faith to implement a lawful alternative where reasonably practicable. Ongo may suspend the affected transfer or processing where necessary to avoid unlawful processing.

8. DATA SUBJECT RIGHTS

8.1 Taking into account the nature of the processing, Ongo shall assist Customer by appropriate technical and organisational measures, insofar as reasonably possible, to enable Customer to respond to requests by Data Subjects exercising rights under Chapter III GDPR or equivalent Applicable Data Protection Law.

8.2 If Ongo receives a Data Subject request relating solely to Personal Data processed on Customer's behalf, Ongo will, where legally permitted, direct the requester to Customer or otherwise notify Customer and will not substantively respond except on Customer's documented instruction or as required by law.

8.3 Customer is responsible for verifying the identity and entitlement of the requester and for determining the substantive response. Material assistance that requires bespoke development, data reconstruction or Professional Services beyond standard Service functionality may be chargeable at agreed rates unless the need for that assistance results from Ongo's breach of the Agreement.

9. DATA-PROTECTION IMPACT ASSESSMENTS AND REGULATORY ASSISTANCE

9.1 Taking into account the nature of processing and the information available to Ongo, Ongo shall provide reasonable assistance to Customer with obligations under Articles 32 to 36 GDPR, including security of processing, Personal Data Breach obligations, data-protection impact assessments and prior consultation, where applicable.

9.2 Ongo may satisfy standard assistance obligations through the Services, Documentation, security information, completed questionnaires, audit reports, certifications, transfer documentation and other existing compliance materials where these reasonably address Customer's request.

9.3 Material additional assistance, bespoke assessments, on-site support, customer-specific evidence packages or regulatory work outside the standard Services may be subject to reasonable Fees agreed in advance, unless the assistance is required because of Ongo's breach of the Agreement or Applicable Data Protection Law.

10. AUDITS AND COMPLIANCE INFORMATION

10.1 Ongo shall make available to Customer information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA. Ongo may initially provide current independent audit reports, certifications, security documentation, policies, questionnaires or other appropriate evidence where these reasonably address the relevant requirement.

10.2 Customer may conduct, or appoint an independent auditor to conduct, an audit or inspection to the extent reasonably necessary to verify compliance with this DPA. Except where a competent supervisory authority requires otherwise, following a material Personal Data Breach, where Customer has reasonable evidence of

material non-compliance, or where another audit is reasonably necessary under Applicable Data Protection Law, Customer will not require more than one audit in any twelve-month period.

10.3 Audits must be preceded by reasonable written notice, take place during normal business hours where practicable, be limited to systems, records and processing relevant to Customer Personal Data, minimise operational disruption, and protect Ongo and third-party Confidential Information, security information and other customers' data. Auditors must be subject to appropriate confidentiality obligations and must not be direct competitors of Ongo unless required by a competent authority.

10.4 Customer bears its own audit costs. Ongo may charge reasonable, documented costs for material assistance beyond standard compliance evidence, provided those charges are not disproportionate or applied so as to make Customer's Article 28 audit right ineffective. Ongo will not charge for reasonable assistance where the audit establishes a material breach of this DPA by Ongo.

10.5 Where an audit identifies a material non-conformity attributable to Ongo, Ongo will take reasonable corrective action appropriate to the risk and the Agreement. Audit findings do not expand Ongo's contractual warranties or liability beyond the Agreement and Applicable Data Protection Law.

11. RETURN, EXPORT AND DELETION

11.1 At the end of the Services involving Processing, Ongo shall, at Customer's choice and subject to the Agreement, return or delete Personal Data and delete existing copies unless Union or Member State law requires storage. The standard export, transition and deletion periods are those stated in the MSA or applicable Order Form, subject to mandatory law.

11.2 Backup or disaster-recovery copies may remain until overwritten or expired in the ordinary backup cycle, provided they remain protected, are not restored except for legitimate continuity, recovery or legal purposes, and are deleted or re-isolated in accordance with the ordinary cycle after any permitted restoration.

11.3 Ongo may retain minimal records that Applicable Data Protection Law or other mandatory law requires Ongo to retain, subject to continued confidentiality and restricted use for the required legal purpose.

12. RESTRICTED AND SENSITIVE DATA

12.1 Customer shall not submit or connect special categories of Personal Data under Article 9 GDPR, Personal Data relating to criminal convictions and offences, data concerning minors, biometric data used for identification, highly sensitive financial information or other specially protected data unless the relevant processing is expressly within the agreed scope and appropriate legal, contractual, technical and organisational safeguards have been confirmed.

12.2 Customer remains responsible for establishing any additional lawful basis, condition, authorisation, professional duty, secrecy obligation, impact assessment or sector requirement applicable to Restricted Data. Ongo may require the relevant processing to be described in an Order Form, Security Schedule or other written addendum before enabling it.

12.3 If Customer introduces materially different or higher-risk Personal Data without the required agreement or safeguards, Ongo may restrict or suspend the affected processing to the extent reasonably necessary to protect the data and maintain compliance while the Parties address the issue.

13. AI, MODEL AND AUTOMATED PROCESSING

13.1 Personal Data processed through AI-enabled functionality, models, agents or automated workflows remains subject to this DPA. Customer's configuration of an AI-enabled use constitutes a documented instruction only within the agreed scope and authority boundaries under the Agreement.

13.2 Ongo shall not use Customer Personal Data to train or improve a general-purpose or cross-customer AI model for Ongo's or a third party's independent purposes without Customer's express written authorisation. This restriction does not prevent processing necessary to provide the contracted inference, orchestration, security or support function in accordance with Customer's documented instructions.

13.3 Where an approved third-party AI or model provider processes Personal Data for the Services, that provider is treated as a Subprocessor to the extent it processes Personal Data on Customer's behalf and is subject to Sections 6 and 7. Ongo will configure or contract with such providers, where reasonably available within the agreed architecture, so that Customer Personal Data is not used to train a general-purpose or cross-customer model without Customer's express written authorisation.

13.4 Nothing in this DPA determines whether an AI model or Output is anonymous, pseudonymous or outside the scope of Applicable Data Protection Law. The Parties will assess such status according to the actual data, processing and legal criteria applicable to the use case.

14. RECORDS, SUPERVISORY AUTHORITIES AND EVIDENCE

14.1 Ongo shall maintain records of categories of processing carried out on behalf of Customer to the extent required by Article 30(2) GDPR and shall make those records available to a competent supervisory authority where legally required.

14.2 Each Party shall cooperate with a competent supervisory authority in accordance with obligations directly applicable to that Party. Where a supervisory authority lawfully requests information from Ongo concerning Customer-controlled processing, Ongo may notify Customer and coordinate the response where legally permitted and reasonably appropriate.

14.3 Ongo may retain compliance evidence, security records and audit trails reasonably necessary to demonstrate performance of this DPA, subject to the Agreement, Applicable Data Protection Law and applicable retention requirements.

15. LIABILITY

15.1 Each Party's liability arising out of or relating to this DPA is subject to the exclusions and limitations of liability in the MSA to the maximum extent permitted by law. This DPA does not create a separate or additional liability cap.

15.2 Where the MSA provides an enhanced cap for data-protection or confidentiality obligations, that enhanced cap applies in aggregate with, and not in addition to, the other caps under the MSA. Nothing in this DPA limits liability to the extent it cannot lawfully be excluded or limited.

16. PRECEDENCE, CHANGES AND DURATION

16.1 If there is a conflict between this DPA and another part of the Agreement concerning Processing of Personal Data, the order of precedence in the MSA applies. An Order Form may specify Customer-specific processing details but does not reduce mandatory data-protection obligations unless lawfully permitted.

16.2 Ongo may update this DPA to reflect changes in law, regulatory guidance, processing or the Services only in accordance with the change provisions of the MSA. A material adverse change affecting Customer's substantive rights during an active Order Term will apply only as permitted by the Agreement or Applicable Data Protection Law.

16.3 This DPA remains in effect for so long as Ongo processes Personal Data on Customer's behalf under the Agreement. Provisions that by their nature apply after Processing ends, including confidentiality, deletion, audit evidence, regulatory cooperation and liability provisions, survive to the extent necessary to give them effect.

ANNEX 1 - DETAILS OF PROCESSING

The following describes the default processing for Ongo Agility. The applicable Order Form may supplement or narrow these details for a specific deployment.

ELEMENT	DEFAULT / ORDER FORM SPECIFICATION
Subject matter	Provision, configuration, hosting where applicable, security, support and operation of Ongo Agility and related Professional Services purchased by Customer.
Duration	For the applicable Order Term and the return, export, transition and deletion period stated in the Agreement, plus any legally required retention period.
Nature of processing	Collection, receipt, access, storage, organisation, retrieval, transmission, consultation, analysis, classification, orchestration, generation, logging, support, deletion and other Processing necessary to provide the Services according to Customer instructions.
Purpose	To provide Customer-requested platform, workflow, collaboration, integration, AI-enabled, automation, reporting, security, support and Professional Services functions.
Categories of Data Subjects	Authorised Users; Customer personnel, contractors and consultants; business contacts; Customer customers, suppliers or partners; and other persons whose Personal Data Customer lawfully places in or connects to the Services.
Categories of Personal Data	Business contact details; account and identity data; roles and permissions; workflow, task and project content; communications and documents; system and integration data; audit, security and usage logs; and other Personal Data Customer elects to process within the agreed scope.

Special categories / Restricted Data	Not intended by default. Permitted only where expressly within the agreed scope and the requirements of Section 12 are satisfied.
Processing frequency	Continuous, periodic or event-driven during the Order Term, as initiated or configured by Customer or necessary to provide and secure the Services.
Customer rights and obligations	Customer determines the lawful purposes of Customer-controlled Processing, issues documented instructions, configures authorised use and exercises controller rights under the Agreement and Applicable Data Protection Law.

ANNEX 2 - BASELINE TECHNICAL AND ORGANISATIONAL MEASURES

These are baseline measures and are applied proportionately to the contracted deployment, service boundary, data and risk. Customer-specific measures or regulated requirements should be stated in the Order Form or Security Schedule.

CONTROL AREA	BASELINE MEASURE
Access control and least privilege	Role-based access controls and administrative permissions designed to limit access according to authorised role and operational need; privileged access is restricted and reviewed proportionately.
Authentication and credentials	Authentication controls appropriate to the Services, support for SSO where included in the purchased configuration, and controls for service credentials, tokens and administrative access.
Encryption	Encryption in transit using current industry-standard protocols and encryption at rest where technically applicable to the agreed hosting model and service component.

CONTROL AREA	BASELINE MEASURE
Logical separation	Logical separation of customer environments or data domains and access-controlled administrative tooling appropriate to the architecture.
Confidentiality and personnel security	Personnel confidentiality obligations, role-based access governance, access removal or adjustment, and security awareness appropriate to personnel responsibilities.
Logging and monitoring	Logging and monitoring designed to identify security-relevant events, support auditability and facilitate incident investigation within the agreed service boundary.

Secure development and change control	Development, deployment, change-management and release practices proportionate to the Services, including controlled changes and separation of development/acceptance/production functions where applicable.
Vulnerability and patch management	Processes proportionate to the Services for identifying, assessing and remediating material vulnerabilities and applying relevant security updates.
Resilience, backup and recovery	Backup, continuity and recovery measures appropriate to the relevant hosting model, including measures designed to restore availability and access in a timely manner following a physical or technical incident.
Incident response	Documented or operational incident-response and escalation procedures designed to contain, investigate, remediate and communicate material security events.
Subprocessor governance	Risk-based due diligence, written data-protection obligations and ongoing management of direct Subprocessors relevant to the Services.
Data minimisation, retention and deletion	Controls and operational practices designed to limit Processing to the contracted purpose and implement retention, export and deletion obligations under the Agreement.
Security testing and evaluation	Processes for periodically testing, assessing or evaluating the effectiveness of relevant technical and organisational measures, proportionate to risk and the maturity of the Services.
Physical and infrastructure security	Physical security and environmental safeguards supplied by Ongo or inherited from approved hosting/data-centre providers appropriate to the deployment model.

ANNEX 3 - SUBPROCESSOR REGISTER AND TRANSFER INFORMATION

The operational register must be completed or linked before external use where Subprocessors process Customer Personal Data. The register may be maintained separately so it can be kept current without reissuing this DPA.

A3.1 Current Subprocessor register: [insert published URL or identify attached/current register].

A3.2 For each relevant Subprocessor, the register should identify, to the extent applicable and reasonably available:

- (a)** legal name and sufficient contact or registered-address information;
- (b)** service and Processing purpose;
- (c)** categories of Personal Data or Processing involved, where useful to understand the role;
- (d)** principal Processing location(s);

- (e) whether the Subprocessor may use onward Subprocessors relevant to Customer Personal Data; and
- (f) where a Chapter V GDPR transfer occurs, the transfer destination and the principal transfer mechanism relied upon.

A3.3 Ongo may provide the information in A3.2 through a web-based trust centre, security portal, subprocessor list, transfer schedule or comparable current record, provided Customer can reasonably access the information during the Order Term.

ANNEX 4 - INTERNATIONAL TRANSFER OPERATING TERMS

A4.1 Where an adequacy decision applies to a relevant recipient and transfer, the Parties may rely on that adequacy decision for so long as it remains valid and applicable to the recipient and Processing.

A4.2 Where SCCs are required, the applicable SCC module is determined by the Parties' actual roles in the transfer. For a transfer from Ongo acting as processor to a non-EEA Subprocessor, the processor-to-processor module will ordinarily apply. Where another module is legally appropriate, the Parties will use that module.

A4.3 The SCCs are not modified by this DPA in a manner that contradicts or restricts the rights and obligations they create. If this DPA conflicts with applicable SCCs concerning the transfer, the SCCs prevail for that transfer to the extent of the conflict.

A4.4 Where required, Ongo as exporter will document the relevant transfer basis, transfer assessment and supplementary measures for transfers it initiates in the processing chain and will make information reasonably necessary for Customer's accountability assessment available in accordance with Section 7.4.

END OF DATA PROCESSING AGREEMENT 2026-27
