Data Processing Agreement

Version 1.0 · Last updated: October 2, 2026
GOSELL (GO SELL) · www.gosell.fr

This Agreement forms part of the contract between GO SELL and the business customer identified in the order. It applies wherever GO SELL processes personal data on the customer's behalf. The completed Processing Schedule, Security Schedule and Subprocessor List form part of this Agreement. They must be available before acceptance and before the corresponding processing starts. This Agreement prevails over inconsistent contractual provisions on data protection; applicable standard contractual clauses prevail in their own scope.

1. Roles and documented instructions

The customer is the controller and GO SELL is the processor for the activities described in the Processing Schedule. The schedule identifies the subject matter, duration, nature and purposes of processing, data types, categories of individuals, and the customer's obligations and rights. Customer instructions consist of this Agreement, the order, the schedules and authorised configuration instructions.

GO SELL processes personal data only on documented instructions, including for transfers, unless Union or Member State law applicable to GO SELL requires processing. In that event, GO SELL informs the customer before processing unless legally prohibited. GO SELL immediately informs the customer if it considers an instruction to infringe applicable data protection law and does not implement that instruction until lawfully resolved.

2. Authorised product processing

For GO VISION and GO VERIFY, source data and analysis stay on the customer's Edge server; the SaaS scope covers only the metadata fields expressly specified in the schedule. Source data remote access is a separate instructed processing operation when authorised. For GO CHECK, GO PERFORM and GO LOYAL in SaaS, processing covers the customer data and features specified in the order. For fully local deployments, the schedule identifies any GO SELL installation, maintenance or support processing and any enabled external connection; no SaaS transfer is presumed.

The customer determines lawful purposes and bases, provides required notices, defines necessary data and retention, and manages its authorised users. It must not instruct unlawful surveillance or prohibited AI uses. GO SELL's own processor obligations remain applicable regardless of customer ownership or control of the data.

3. Confidentiality and security

GO SELL ensures that persons authorised to process data are bound by confidentiality and have access only as necessary. It implements the measures required by Article 32 GDPR and described in the Security Schedule. The parties specify responsibility for infrastructure, backup, recovery, updates, remote access and credentials. GO SELL secures its own accounts and operations even where the underlying server belongs to the customer.

Support access must be authorised, limited to the relevant task, appropriately logged and withdrawn when no longer needed. Customer administrator passwords must not be requested for routine support. Any exceptional access to source content must be documented and limited to the agreed purpose.

4. Subprocessors and transfers

The customer grants general written authorisation to the subprocessors identified in the Subprocessor List available at acceptance. GO SELL gives at least 30 days' advance notice of a proposed addition or replacement that will process customer data. The customer may object on documented data protection grounds. The parties seek a compliant alternative; if none is available, the affected processing is not entrusted to that provider and the parties arrange suspension or termination of the affected service under the contract. No emergency removes the requirement for lawful authorisation and appropriate safeguards.

GO SELL imposes equivalent data protection obligations on each subprocessor and remains responsible to the customer for its performance. Storage, backup and access locations, and international transfer mechanisms, are documented. Transfers outside the EEA require documented instructions and compliance with Chapter V GDPR. A local AI deployment does not authorise an undisclosed external model service.

5. Assistance and individual rights

Taking account of the nature of processing and the information available, GO SELL assists the customer with individual rights requests, security, breach handling, impact assessments and prior consultation under Articles 32 to 36 GDPR. GO SELL forwards requests concerning customer data and does not decide them independently unless legally required. Any agreed assistance charges must be transparent and must not prevent mandatory compliance.

6. Personal data breaches

GO SELL notifies the customer without undue delay after becoming aware of a personal data breach affecting entrusted data. The initial notice is not delayed until an investigation is complete. It includes available information on the nature of the incident, affected data and people, approximate volumes, contact point, likely consequences and measures taken or proposed. Further information is supplied progressively, and GO SELL preserves relevant evidence and cooperates with the customer.

The customer determines its notifications to authorities and individuals. The controller's 72-hour notification rule is not the processor's notification period. GO SELL communicates on the customer's behalf only on instruction or as required by law.

7. Demonstrating compliance and audits

GO SELL makes available the information necessary to demonstrate compliance with Article 28 GDPR and allows and contributes to audits and inspections by the customer or its mandated auditor. Reasonable arrangements may protect confidentiality, other customers and service availability without undermining the audit right, including in an incident or supervisory inquiry. GO SELL informs the customer of a relevant compliance deficiency and cooperates in addressing it.

8. Return and deletion

At the end of the processing services, GO SELL returns or deletes the personal data at the customer's choice and deletes existing copies unless applicable law requires storage. The Processing Schedule specifies the export format, recovery window, operational deletion deadline and maximum backup expiry period. Residual backup data remain protected, are not used for routine operations and expire on the documented cycle; required deletions are reapplied following restoration. GO SELL confirms completion on request.

For data remaining on customer infrastructure, the customer performs the deletion operations assigned to it; GO SELL deletes any copies it holds. Retained statutory data are segregated and used only for the legal purpose. Applicable Data Act switching rights and contractual exit provisions operate separately from GDPR portability and must be respected where the service falls within their scope.

9. Responsibility and changes

This Agreement does not limit the rights of individuals, supervisory powers or liabilities imposed by Article 82 GDPR. It does not authorise GO SELL to use entrusted data for its own unrelated purposes. An independent purpose requires a separate lawful framework and appropriate information. Material changes are notified and agreed where necessary; instructions and accepted versions remain traceable.

10. Processing Schedule

The customer-specific order or attached schedule must record: customer identity and contacts; selected product and deployment; purpose and duration; processing operations; categories of data and people; any special-category or offence data and restrictions; exact metadata fields; authorised source-data access; integrations and AI providers; storage, backup and support countries; transfer safeguards; retention by category; export formats and retrieval window; production and backup deletion deadlines; incident contacts; and the applicable Security Schedule and Subprocessor List versions. Only the completed schedule associated with the order is contractually applicable.

11. Security Schedule

The service-specific schedule records verified measures and responsibilities for user and privileged access, authentication, confidentiality, tenant separation where applicable, protection in transit and at rest, key management where applicable, logging, updates and vulnerability handling, incident response, backup and restoration, remote support, and Edge security. It identifies any customer-operated components and expressly states any backup service included or excluded. The schedule is provided as part of the accepted service documentation.