Privacy Policy

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

This Privacy Policy explains how GO SELL uses personal data relating to its website, business contacts and services. The Data Processing Agreement in section B governs personal data processed on behalf of a business customer. Commercial terms, prices, licence rights and service levels are governed by the applicable Terms of Sale and Service.

1. Who is responsible for your data

GOSELL, trading as GO SELL, is the controller for personal data used to manage www.gosell.fr, enquiries, its commercial relationships, orders and its own business administration. You can contact us at protection-vie-privee@gosell.fr or write to GO SELL, 52 rue de Sablonville, 92200 Neuilly-sur-Seine, France.

For personal data that an organisation processes through our products for its own purposes, that organisation is normally the controller. GO SELL acts as its processor to the extent that it hosts, accesses or otherwise processes that data on its instructions. Customer control of data and passwords does not remove GO SELL’s obligations as a processor. A fully local installation does not by itself establish whether GO SELL is a processor: the actual processing and access arrangements determine the role.

2. Product architecture and data flows

GO VISION and GO VERIFY use an Edge server on the customer’s infrastructure. Source video, images and documents, and their analysis, remain local. Only metadata are transferred to the SaaS service. Metadata can include events, timestamps, technical identifiers, measurements and analysis results, depending on the enabled features. The service configuration defines the exact fields and permitted purposes. Metadata remain personal data whenever an individual can be identified, directly or indirectly.

Source video, images, documents and prompts containing source content must not be sent to the SaaS service as “metadata”. Any separately requested remote access to source data requires documented customer instructions and appropriate safeguards; it is not authorised by the standard metadata transfer.

GO CHECK, GO PERFORM and GO LOYAL provide a SaaS platform on which the customer enters and administers its business data, manages authorised users and sets access credentials. Depending on the subscribed module, these data can include audit records and photographs, employee and applicant information, skills and training records, or customer feedback. Access is governed by the customer’s authorised roles and the agreed support arrangements.

All solutions may also be deployed entirely on the customer’s infrastructure under an agreed local deployment. In that configuration, SaaS transfers are not required by the deployment itself. Any enabled connection, integration or support access must be described in the service configuration. Local storage, backups and infrastructure operations are assigned to the customer unless the service agreement expressly assigns a task to GO SELL.

For a SaaS deployment, the service documentation provided before business data processing starts identifies the hosting and backup locations, authorised processing providers, support access countries and any international transfer safeguards. Local AI processing does not require transmission of source data to an external model provider. Any external AI service used for SaaS metadata or other SaaS data must be identified and covered by the agreed processing terms before it is enabled.

3. Personal data collected for our own purposes

We collect information you provide, such as name, professional email address, telephone number, employer, job title and enquiry content. We also process account identifiers, order and subscription information, billing details, transaction status, support correspondence, privacy preferences and relevant connection and security records. Mandatory fields are identified when collected; without them, we may be unable to fulfil an order or respond to your request.

Data can also come from your organisation, an authorised business partner or a lawful professional source. Where Article 14 GDPR applies, we provide the required information, including categories and source, within the applicable period, normally no later than one month, the first communication or the first disclosure, whichever applies, unless a lawful exception applies.

The checkout identifies the payment provider and links to its privacy information. The provider processes payment details within its own role. GO SELL uses the transaction information necessary to manage the order and invoicing. Do not send full card details to our support team. Any card token or payment reference used for recurring billing is subject to the payment integration disclosed at checkout.

4. Purposes and legal bases

Enquiries, quotations and orders: we use the details needed to respond and supply the requested service. The legal basis is steps requested before a contract or contractual necessity when the individual is a contracting party. For employees representing a business customer, the basis is our legitimate interest in managing the business relationship.

Account administration and support: we use relevant identification, contact and service information to administer access and handle requests. Contractual necessity applies to individual contracting customers; our legitimate interest in operating the service and assisting the customer applies to its business representatives. Processing of customer business data is governed by section B, and the customer determines its applicable legal basis.

Invoicing and statutory records: we process billing and accounting data to meet legal obligations. Fraud prevention, proportionate security monitoring and legal claims: we process the necessary records on the basis of legitimate interests, subject to balancing against individual rights, or a legal obligation where specifically applicable.

Business marketing: where permitted, we contact professional recipients about services relevant to their role on the basis of legitimate interests, with clear information and a free right to object. We obtain consent whenever required. We do not use the business data entrusted to us in our products to market to a customer’s employees or customers. Each marketing email provides an unsubscribe mechanism.

Optional cookies and similar technologies: consent where required. Strictly necessary technologies are used within the applicable exemption. Neither acceptance of contractual terms nor payment constitutes consent to optional marketing or tracking.

5. Recipients and international transfers

Access is limited to authorised personnel and providers that need the data for the relevant service: hosting, maintenance, communications, payment and any enabled AI processing. Providers are subject to obligations appropriate to their roles. Independent controllers, such as a payment provider acting in that capacity, also provide their own privacy information. Advisers and competent authorities may receive necessary data where a lawful obligation or justified legal need applies. GO SELL does not sell personal data.

Our Subprocessor List identifies the legal entities processing customer business data, their tasks, relevant storage and access countries, and transfer arrangements. It is made available with the applicable service

documentation. An EU storage location does not exclude an international transfer where data are accessed from outside the European Economic Area.

Transfers outside the EEA must satisfy Chapter V GDPR. They rely on an applicable adequacy decision or appropriate safeguards, including European Commission standard contractual clauses where relevant, supported by the required assessment and supplementary measures. Reliance on the EU–US Data Privacy Framework requires a currently certified recipient and a covered processing activity. You may request information and a relevant copy of the safeguards, subject to protection of confidential information and third-party rights.

6. Retention

We retain data only for the relevant purpose and applicable legal periods. Data required for a legal obligation or dispute are placed in restricted archives rather than kept in routine operational use. Pseudonymisation does not replace deletion or effective anonymisation.

Marketing prospects: up to three years from collection or the last contact initiated by the prospect. Customer contact data used for marketing: during the business relationship and up to three years after its end or the last relevant contact. Minimal suppression records are retained for at least three years and longer where needed to respect an objection and prevent renewed contact.

Invoices and accounting records: ten years from the end of the relevant financial year. Contracts and evidence: for the relationship and then the applicable limitation period, generally five years for commercial obligations, subject to a different statutory period or an ongoing claim.

Account data remain active while needed to administer the account or contract; after closure, only data necessary for outstanding obligations, evidence or security are retained under the relevant criteria above. Support records are retained while a request is handled and thereafter only to the extent needed to resolve the issue, fulfil obligations or document a claim. Security records are retained according to the detection and investigation window justified by the system risks; an identified incident or claim may require restricted retention of relevant records. Cookie durations and choice retention are stated in the Cookie Policy.

Customer business data, metadata and backups follow the retention instructions in the service schedule. Video, documents, HR records and metadata must each have a justified retention rule. Source data on a local server follow the customer’s configuration. SaaS retention and deletion, including backup expiry, are specified in the applicable service schedule. GO SELL does not select a universal retention period for every customer business purpose.

7. Security and incident handling

GO SELL must implement technical and organisational measures appropriate to its processing risks under Article 32 GDPR. The service security schedule describes the applicable access restrictions, confidentiality arrangements, communication protection, vulnerability management, logging, backup and recovery responsibilities, and incident procedures. Measures must reflect the actual deployment; this policy does not claim a certification, a particular encryption algorithm or an absolute security guarantee.

Customer administrators manage the users and access rights under their control and must protect their credentials. GO SELL remains responsible for its own authorised access, operations and providers. Local infrastructure responsibilities do not authorise uncontrolled support access.

Where GO SELL becomes aware of a personal data breach involving data processed for a customer, it notifies that customer without undue delay and provides information progressively as it becomes available. Where GO SELL is the controller, it assesses and fulfils its own notification obligations, including notification to the supervisory authority within 72 hours where required and communication to individuals where the legal

criteria are met.

8. AI and video safeguards

AI features may generate analyses, alerts, summaries, forecasts or recommendations. They can make mistakes. An AI interaction is clearly identified, and outputs must be checked before use in a decision affecting a person. A customer must not implement a solely automated decision with legal or similarly significant effects unless the conditions and safeguards of Article 22 GDPR are met.

GO SELL does not obtain permission through this policy or an order to train models for its own purposes on customer business data. Nor does an order authorise a model provider to reuse those data. Any separate training or reuse project requires a documented lawful framework, appropriate transparency and any legally required consent. Customer agreement does not substitute for a person’s consent when that consent is required.

The customer must ensure lawful and proportionate video and HR uses, inform the people concerned, comply with employment and video protection rules, consult employee representatives where required, and conduct a data protection impact assessment where required. Existing cameras do not automatically authorise AI analysis. Permanent and disproportionate employee surveillance is excluded. Emotion recognition in workplaces or educational institutions and prohibited biometric categorisation may not be enabled except where the law expressly permits the relevant use. Biometrics, sensitive data and employment-related AI require specific assessment before activation. Local processing does not exempt a use from these rules.

9. Your rights and how to exercise them

Subject to the statutory conditions, you have rights of access, rectification, erasure, restriction and objection. Portability applies to automated processing based on consent or contract. You may withdraw consent at any time without affecting the lawfulness of earlier processing. You may object to direct marketing at any time. Under French law, you may also provide instructions concerning your personal data after death.

Contact protection-vie-privee@gosell.fr or the postal address above. We seek additional identity information only where there is reasonable doubt and only to the extent necessary. We normally respond within one month of receiving the request. If complexity or number of requests justifies an extension of up to two further months, we explain it within the first month. Requests are normally free, subject to the statutory exceptions.

For data processed on behalf of your employer or another customer organisation, that organisation decides how to respond. You can contact it directly; if we receive the request, we pass it to the customer and assist within our role. You can complain to the French supervisory authority, CNIL, at www.cnil.fr, or to another competent authority, without first contacting us.

10. Cookies and updates

Optional technologies requiring consent are not activated before a valid choice. Rejecting them is as easy as accepting them and does not prevent purchase. The Cookie Policy and the permanent Manage cookies control explain purposes, providers, durations and relevant transfers and allow choices to be changed.

The current version and date appear on this policy. We provide appropriate notice of material changes. A new purpose does not become lawful simply because an updated policy is published; further information and fresh consent are provided where required.