



Introduction and scope

Renato Software Ltd and Senso.cloud, together referred to in this Privacy Notice as "Renato", "Senso", "Senso.cloud", "we", "us" and "our", are committed to protecting privacy and handling personal data responsibly.

This Privacy Notice explains how we process personal data when we act as a controller for our own business and website activities, and how we process service data when we act as a processor or service provider for our customers.

This Notice applies to customers that subscribe to Senso.cloud services and to individuals whose personal data we collect for our own purposes. It does not replace a customer organisation's own privacy notices to its users, pupils, staff or end users.

Roles and terminology

TERM	MEANING
Collected Data	Personal data we collect and process for our own purposes, such as account administration, billing, marketing, website analytics, events, enquiries and customer relationship management. For Collected Data, Renato Software Ltd is generally the controller.
Service Data	Electronic data, text, messages, materials and personal data submitted to or collected through the Senso.cloud services by or on behalf of a customer. For Service Data, the customer is generally the controller and Senso.cloud acts as processor/service provider.
User / End-User	Individuals who use or are monitored through the services under a customer account, including school staff, pupils or other authorised users, depending on the deployment.
Customer	The organisation that subscribes to, configures and controls use of the Senso.cloud services.

Collected Data we process for our own purposes

We may collect and process Collected Data in the following circumstances.

Sign-up, billing and account information

When a customer subscribes or signs up for services, we may collect contact information such as name, email address, mailing address, IP address, geographic location and telephone number for account administrators; billing information such as payment details and billing address; feedback submitted from within the services; and identifiers such as username, account number or password. We use this information to provide the services, communicate about the services, administer accounts, respond to support requests, assess customer needs, provide requested information, facilitate transactions and send marketing communications where requested or permitted.

Events

When individuals attend events such as webinars or seminars, we may collect name, email address, job title and company name. We use this to respond to questions, provide requested information, assess customer needs and send marketing communications where requested or permitted.

Referrals

Customers may provide contact details for referrals, such as name, email address, mailing address or telephone number. Customers providing third-party referral information must ensure they have the lawful right to do so and have provided appropriate notice or obtained necessary consent. We use referral data to assess service needs, respond to enquiries and send marketing communications where requested or permitted.

Trial registrations

When an individual registers for a trial through our websites, we may collect name, email address, company name, website URL, company details, location and contact information. We use this information to facilitate the trial, provide service communications, respond to requests and send marketing communications where requested or permitted.

Public forums, forms and newsletters

When individuals submit website forms, participate in publicly accessible community forums or blogs, or subscribe to newsletters, we may collect contact details, business information and author profile information. Information posted in public forums may be read, collected and used by others. Newsletter email addresses are used to provide updates and related communications.

Cookies and similar technologies

We and our partners may use cookies and similar technologies to analyse trends, administer websites, track user movement, gather demographic information and improve website and service performance. Browser settings can usually be used to control cookies, although disabling cookies may limit functionality.

Analytics

When individuals visit our websites or use our services, we may automatically receive information such as device model, IP address, browser type, usage patterns through cookies and browser settings, query logs, product usage logs, clicks, scrolls, conversions and drop-off information. We use analytics to improve, enhance, support and operate our websites and services, assess customer needs and compile statistical insights.

Testimonials

We may publish testimonials, comments or reviews that contain personal data, but we will obtain consent before publishing a person's name with a testimonial. Requests to remove testimonials can be sent to support@renatosoftware.com.

Marketing communications

Where permitted or requested, we may use email addresses and other Collected Data to send newsletters or marketing communications about Senso.cloud products, services or partners. Recipients may opt out using unsubscribe instructions in emails or by contacting us.

Legal basis for processing Collected Data

Where UK GDPR, EU GDPR or equivalent data protection law applies, our legal basis depends on the specific personal data and context. We normally collect and use personal data where processing is necessary to perform a contract, where processing is in our legitimate interests and not overridden by individual rights and freedoms, where consent has been provided, where required by law, or where necessary to protect vital interests.

Where information is required to enter into or perform a contract, or to comply with a legal obligation, we will make this clear where appropriate. Where we rely on legitimate interests, we will identify those interests where required.

Service Data we process on behalf of customers

We process Service Data only in accordance with customer instructions, the customer agreement and applicable law. For GDPR purposes, customers are generally controllers of Service Data and Senso.cloud is generally the processor.

Service Data includes electronic data, text, messages, materials and personal data of users and end-users submitted to or collected through the services by customers through their accounts. This may include information collected through product logs and service functionality, depending on the selected Senso.cloud modules and configuration.

We do not own, control or direct the use of Service Data. We are largely unaware of the specific content customers store or process through the platform and only access Service Data as reasonably necessary to provide and support the services, as authorised by the customer, or as required by law.

Customers are responsible for providing appropriate notices to users and end-users, obtaining any required consents or authorisations, configuring the services lawfully, and determining how Service Data should be used, accessed and retained.

Other information processed through the services

When a user or end-user uses the services, we may automatically receive and record information such as device model, IP address, browser type, usage pattern through cookies and browser settings, query logs and product usage logs. We process this information to provide, improve, enhance, support and operate the services and their availability, develop new products and services, and compile statistical reports and usage insights.

Single sign-on

Users may log in to Senso.cloud services or websites using sign-in services such as Google and Microsoft. Those services authenticate the user and may provide the option to share personal data with us, such as name and email address.

Sharing personal data

We may share personal data with third parties where necessary to provide, support, operate, improve or administer our services and business, subject to confidentiality and appropriate safeguards.

- Third-party providers assisting us in providing the services, including subprocessors with access to customer accounts or Service Data only as reasonably necessary to provide the services.
- Third-party service providers that provide research, analytics, marketing, data enrichment or communications services on our behalf.
- Payment processors that process credit card and payment information and are not permitted to use that information for unrelated purposes.
- Partners who assist with customer onboarding and service support.
- Sponsors of contests or events where the individual registers for that contest or event.
- Social media networks, advertising networks and websites where relevant to website or marketing activities.
- Potential or actual acquirers, investors or advisers in connection with a merger, reorganisation, acquisition, sale of assets, due diligence exercise or similar corporate transaction.
- Public authorities, regulators, courts, law enforcement or other parties where disclosure is required by law or reasonably necessary to protect rights, safety or security.

Subprocessors and external service providers

The following service providers are identified in our privacy and assurance materials. The list may be updated from time to time as services and vendors change.

VENDOR	PURPOSE	LOCATION / DATA CENTRE INFORMATION	RELEVANT PRODUCTS / SERVICES
Microsoft Azure	Primary cloud infrastructure provider for Senso.cloud SaaS applications and storage/processing of most service data.	European Economic Area for relevant UK/EU services; Azure Australia regions for Australian customer Service Data where provisioned for Australian tenancies.	Senso Enterprise, Class, Network, Safeguarding/Safeguard, Asset and related cloud services.
Stripe Inc.	Payment transactions and payment platform services.	Stripe-hosted payment processing locations and safeguards.	Stripe Connect / payment services.
SendGrid Inc.	Managed email service used for application-generated email communications.	United States.	Senso.cloud application email services.
Microsoft Dynamics 365	CRM, marketing, finance, ERP, productivity and business management activities.	European Economic Area.	CRM, marketing, finance, ERP and AI-enabled business functions.
Freshworks Ltd.	Customer engagement and support tooling.	European Economic Area.	FreshSales, FreshDesk and FreshChat.
Xero Ltd.	Accounting and finance services.	Xero uses cloud infrastructure including AWS services; appropriate transfer safeguards are applied where required.	Accounting services.

International transfers

Personal data may be processed in the United Kingdom, European Economic Area and other countries where we or our service providers operate. Where personal data is transferred internationally, we use appropriate

safeguards required by applicable law, which may include adequacy decisions, contractual commitments, standard contractual clauses, data minimisation, access controls and security measures.

Information obtained from third parties

We may receive personal information from third-party sources such as databases and social media, but only where we have checked that those third parties have consent or are otherwise legally permitted or required to disclose the information. This may include name, email address, postal address, location, designation and telephone number. We use this information to maintain and improve customer support, improve the accuracy of our records, and support sales and marketing activities.

Security measures

We use appropriate technical and organisational measures designed to provide a level of security appropriate to the risk of processing personal data. Security risks and controls are reviewed periodically as part of internal and external assurance activities.

Data in transit and at rest

- Senso.cloud uses industry-standard protocols to encrypt data in transit between devices and Microsoft datacentres used to host Senso.cloud services.
- Azure security capabilities include protection for data in transit and at rest, including encryption for data, files, applications, services, communications and drives.
- Encryption mechanisms include SSL/TLS, IPsec and AES, as applicable to the service layer.
- Access to stored data by Microsoft Azure support personnel requires explicit Senso.cloud permission, is granted on a just-in-time basis, is logged and audited, and is revoked after the engagement.

Senso.cloud platform security

- TLS encrypted communications are used for platform data communication.
- Console access rights are applied to individual console users.
- Senso.cloud databases are IP restricted to authorised office locations and administrative access paths.
- Backend Azure configuration and tenancy administration are protected by two-factor authentication.
- Data access is time-limited, limited to authorised users and restricted to the lowest practicable level of access.
- Auditing is enabled on Senso.cloud databases.
- Microsoft Threat Detection / Defender capabilities are enabled on Senso.cloud databases where applicable.
- Senso.cloud staff do not have master accounts that can be used to access customer accounts.
- Senso.cloud modules are hashed and only modules with the correct hash are allowed to run.
- Customer portal access by Senso.cloud support personnel requires explicit customer permission, is just-in-time, is logged and audited in the customer console, and is revoked after completion.
- Access to customer data for support is read-only where applicable and cannot be tampered with by users at the customer organisation.
- Devices require approval before being shown in the Senso.cloud portal.

Individual rights for Collected Data

Where applicable data protection law grants rights over personal data, individuals may have the right to access, correct, update, delete, object to, restrict processing of, request portability of, or withdraw consent for their personal data. Individuals may also opt out of marketing communications at any time and may complain to a data protection authority.

Requests concerning Collected Data can be made by contacting us at support@renatosoftware.com. We respond to requests within a reasonable timeframe and in accordance with applicable data protection laws.

Requests concerning Service Data

Because Senso.cloud processes Service Data on behalf of customers, individuals seeking access to, correction of, deletion of or other rights in Service Data should contact the relevant customer organisation, which is generally the controller of that data. Where a customer asks us to assist with a valid request concerning Service Data, we will respond within a reasonable timeframe and in accordance with our agreement and applicable law.

Customers may raise Service Data requests through the relevant Senso.cloud support portal or account process.

Service communications

Customers may receive non-promotional service announcements where necessary, for example notices about maintenance, security, support or service availability. These operational communications are generally not optional while an account is active.

Retention of personal data

Collected Data is retained for as long as necessary for the purposes described in this Notice, unless a longer retention period is required or permitted by law. Individuals may request that we no longer use their Collected Data by contacting support@renatosoftware.com.

Personal data contained in Service Data is retained and deleted in accordance with the customer agreement, applicable product settings and the relevant retention policy. We may retain Collected Data and Service Data where necessary to comply with legal obligations, maintain accurate financial and business records, resolve disputes, enforce agreements, or for litigation and defence purposes.

Third-party websites

Our websites may contain links to websites not owned or controlled by Renato Software Ltd. We are not responsible for the privacy practices of those websites or third parties. Individuals should review the privacy policies of external websites they visit.

Children's personal data

Renato Software Ltd does not knowingly collect personal data from children under the age of 16 through our public website. Children under 16 should not submit personal data through our website. Parents and guardians are encouraged to monitor children's internet use and to instruct children not to provide personal data through our website without permission.

Where Senso.cloud services are used by schools or other customers in relation to pupils or children, the customer is responsible for determining the lawful basis, providing notices and obtaining any required consents or authorisations for the processing of Service Data.

Legal disclosures and business transitions

We may disclose personal data contained in Collected Data or Service Data where required by applicable law, in response to lawful requests by public authorities, including national security or law enforcement requirements, or

where disclosure is necessary to protect our rights or comply with judicial proceedings, court orders or legal process.

If Renato Software Ltd undergoes a business transition such as a merger, acquisition or sale of assets, customer accounts, Collected Data and Service Data may be transferred as part of that transaction. We will use reasonable efforts to provide notice of material changes in ownership or control where required by law.

Regional addenda

Additional regional privacy provisions may apply in certain jurisdictions. For Australian customers and end-users, including K-12 schools and school systems using Senso.cloud services in Australia, the Senso.cloud Privacy Notice - Australia Addendum forms part of this Privacy Notice and applies alongside it.

Contacting Senso.cloud

Questions about this Privacy Notice or privacy matters can be sent through our website at <https://www.senso.cloud/contact-us/> or by contacting support@renatosoftware.com.

Postal contact: Renato Software Ltd, Bell House, Wheatcroft Business Park, Landmere Lane, Edwalton, Nottingham, NG12 4DG, United Kingdom.