RAVN PRIVACY POLICY

Last Updated: May 3, 2026

Ravn ("we," "our," or "us") is committed to protecting your privacy and maintaining the trust of every individual and organization that interacts with our platform. Ravn is an AI-native operating system designed to build and run AI-native service firms. Because of the nature of our platform — which involves orchestrating intelligent agents, automating business workflows, and processing operational data on behalf of service firms — we take our data responsibilities seriously. This Privacy Policy explains in detail how we collect, use, store, share, and protect your information when you access or use Ravn and any of its associated products, services, APIs, or interfaces (collectively, the "Service"). By using the Service, you agree to the terms of this Privacy Policy. If you do not agree, please discontinue use of the Service immediately.

INFORMATION WE COLLECT

We collect several categories of information to power the Ravn platform and deliver a reliable, intelligent, and secure experience for you and your organization.

1.1 Account and Identity Data

1.2

When you create a Ravn account or onboard your firm onto the platform, we collect information such as your full name, business email address, job title, company name, and login credentials. For organizations, we may also collect billing information, tax identification numbers, and details about authorized administrators and users within your firm.

1.3 Operational and Workflow Data

Because Ravn is designed to build and run AI-native service firms, we collect data generated by the workflows, automations, and AI agents you configure and deploy through the platform. This includes task inputs and outputs, instructions passed to AI agents, workflow logic and configurations, service delivery records, and the results of automated processes executed on your behalf. This data is essential to the core function of the Service and is handled with strict confidentiality.

1.3 Usage and Interaction Data

We collect detailed information about how you interact with the Ravn platform. This includes which features you access, how frequently you use them, the sequence of actions taken within sessions, time spent on specific modules, errors or failures encountered, and any feedback or support requests submitted. This data helps us improve the platform, identify performance bottlenecks, and personalize your experience.

1.4 AI Model Interaction Data

When you interact with AI agents, assistants, or generative features within Ravn, we may process the prompts, instructions, and contextual inputs you provide, as well as the outputs generated in response. This data is used to deliver the AI functionality you have requested and, where applicable and with your consent, to improve the quality and reliability of our AI systems.

1.5 Technical and Device Data

We collect technical information about the devices, browsers, and network environments used to access Ravn. This includes IP addresses, operating system type and version, browser type and version, device identifiers, screen resolution, language settings, and connection data. This information is used for security monitoring, platform compatibility, and performance optimization.

1.6 Integration and Third-Party Service Data

If you connect Ravn to external tools, platforms, or data sources — such as CRMs, communication tools, cloud storage, or other business software — we may collect and process data from those

integrations to the extent necessary to execute the workflows you configure. You are responsible for ensuring you have the appropriate rights to connect and share such data with Ravn.

1.7 Communications Data
If you contact our support team, respond to surveys, participate in beta programs, or communicate with us through any channel, we retain records of those communications to provide support and improve our services.

1.8 What We Do Not Collect
We do not collect sensitive personal information such as government identification numbers, financial account credentials, health records, or biometric data unless explicitly required by a specific feature you have opted into, and only with clear notice and consent.

HOW WE USE YOUR INFORMATION

We use the information we collect for a range of purposes, all of which are tied to operating the Ravn platform safely, effectively, and in a way that genuinely serves you and your organization.

2.1 Service Delivery and Operation
The primary use of your data is to deliver the functionality you have signed up for — orchestrating AI agents, running automated service workflows, managing firm operations, and providing the analytical dashboards and reporting tools built into the platform.

2.2 Personalization and Experience Improvement
We analyze usage patterns and operational data to tailor the platform to your preferences, surface relevant features, recommend workflow optimizations, and reduce friction in your day-to-day use of the Service.

2.3 AI System Development and Improvement
Where permitted and subject to your choices, we may use de-identified or aggregated interaction data to train, evaluate, and improve the AI models and agent behaviors that power the Ravn platform. We will always provide clear mechanisms to opt out of this use.

2.4 Security, Integrity, and Abuse Prevention
We use technical and usage data to monitor for unauthorized access, detect anomalous behavior, protect against fraud and abuse, enforce our terms of service, and ensure the integrity of the platform and your firm's data.

2.5 Communications and Notifications
We use your contact information to send transactional messages such as account confirmations, security alerts, and invoicing, as well as product updates and, where you have opted in, information about new features or services that may be relevant to your firm.

2.6 Legal and Compliance Obligations
We may process your data to comply with applicable laws, respond to lawful requests from regulatory authorities, and enforce our contractual rights and obligations.

2.7 Internal Business Operations
Aggregated, anonymized data may be used for internal business analysis, strategic planning, investor reporting, and benchmarking. This data is stripped of personally identifying information before such use.

SHARING OF INFORMATION

Ravn does not sell, rent, or trade your personal data or your firm's operational data to any third party for marketing or commercial purposes. We treat the data you entrust to us with the same care we would expect for our own.

3.1 Service Providers and Infrastructure Partners

We work with carefully selected third-party vendors to provide hosting, cloud infrastructure, data analytics, customer support tools, payment processing, and security services. These providers are contractually bound to use your data only as necessary to perform services on our behalf and are required to maintain appropriate data protection standards.

3.2 AI and Model Providers

Certain AI capabilities within the Ravn platform may be powered by third-party AI providers or foundation model vendors. Where your data is passed to such providers to fulfill a request you have initiated, we ensure appropriate data processing agreements are in place and that your data is not used by those providers to train their own models without your explicit consent.

3.3 Business Transfers and Corporate Transactions

In the event of a merger, acquisition, restructuring, or sale of all or a portion of our assets, your data may be transferred to the acquiring entity. We will notify you in advance of any such transfer and, where required by law, obtain your consent.

3.4 Legal and Regulatory Disclosure

We may disclose your information if required to do so by law, court order, governmental regulation, or in good faith belief that such disclosure is necessary to protect the rights, property, or safety of Ravn, our users, or the public.

3.5 Disclosure With Your Consent

We may share your information with third parties in other circumstances where you have provided your explicit, informed consent. We do not grant third parties the right to use your data for their own independent purposes without your knowledge and agreement.

DATA STORAGE, RETENTION, AND SECURITY

4.1 Storage and Infrastructure

Your data is stored on secure cloud infrastructure operated by reputable providers with industry-standard physical, technical, and administrative safeguards. We use encryption at rest and in transit, access controls, and regular security audits to protect your information.

4.2 Data Retention Schedules

We retain your account and operational data for as long as your account is active or as necessary to provide the Service. If you close your account, we will delete or anonymize your personal data within a reasonable period, except where retention is required to comply with legal obligations, resolve disputes, or enforce our agreements. Specific retention schedules are available upon request.

4.3 Security Practices and Controls

We implement a range of technical and organizational measures to safeguard your data, including role-based access controls, multi-factor authentication requirements, intrusion detection systems, encrypted backups, and regular vulnerability assessments. Despite these measures, no system is entirely immune to risk, and we cannot guarantee absolute security.

4.4 Breach Notification

In the event of a data breach that affects your personal information, we will notify you in accordance with applicable law, including within the timeframes required by GDPR and other relevant regional regulations.

4.5 Data Residency

Depending on your location and the configuration of your firm's account, your data may be stored and processed in multiple jurisdictions. Where required by law, we offer data residency options that allow you to specify the geographic region in which your data is held.

CHILDREN'S PRIVACY

5.1 Age Restrictions

The Ravn platform is a professional, enterprise-grade service designed exclusively for use by adults operating or working within service firms and business organizations. Ravn is not intended for, directed at, or designed to be used by individuals under the age of 16, or under the age of 18 in jurisdictions where that is the applicable minimum.

5.2 Collection From Minors

We do not knowingly collect personal data from minors. If you believe that a minor has submitted personal information through our platform, please contact us immediately and we will take prompt steps to delete the information.

YOUR RIGHTS AND CHOICES

Depending on your location and applicable privacy laws — including the General Data Protection Regulation (GDPR) for users in the European Economic Area, the UK GDPR, the California Consumer Privacy Act (CCPA), and other regional frameworks — you may have the following rights with respect to your personal data.

6.1 Right of Access

You may request a copy of the personal data we hold about you and receive information about how it is being processed, including the purposes of processing, the categories of data involved, and the recipients to whom it has been disclosed.

6.2 Right to Rectification

You may request that we correct any inaccurate or incomplete personal data we hold about you. We will act on such requests promptly and notify any relevant third parties of the correction where appropriate.

6.3 Right to Erasure

You may request that we delete your personal data where it is no longer necessary for the purposes for which it was collected, where you have withdrawn consent, or where no other legal basis for processing applies. Certain exceptions may apply where retention is required by law.

6.4 Right to Restriction of Processing

You may request that we restrict the processing of your personal data in certain circumstances, such as while a dispute about accuracy is being resolved or while an objection to processing is being considered.

6.5 Right to Data Portability

Where processing is based on your consent or the performance of a contract, you may request that we provide your personal data in a structured, commonly used, machine-readable format so that it can be transferred to another provider.

6.6 Right to Object

You may object to the processing of your personal data where processing is based on our legitimate interests, including for direct marketing purposes. We will cease processing unless we can demonstrate compelling legitimate grounds that override your interests.

6.7 Right to Withdraw Consent

Where we rely on your consent to process your data, you may withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

6.8 Rights Related to Automated Decision-Making

If Ravn uses automated processes to make decisions that have a significant effect on you, you have the right to request human review of those decisions, to contest the outcome, and to receive a meaningful explanation of the logic involved.

6.9 How to Exercise Your Rights

To exercise any of these rights, please contact us using the details provided in Section 9 below. We will respond to all verifiable requests within the timeframes required by applicable law. In some cases, we may need to verify your identity before fulfilling a request. We will not discriminate against you for exercising any of these rights.

COOKIES AND TRACKING TECHNOLOGIES

7.1 Types of Cookies We Use

Ravn uses cookies, pixels, and similar tracking technologies to operate the platform, remember your preferences, analyze usage patterns, and improve our services. These include strictly necessary cookies required for the platform to function, performance cookies that help us understand how users interact with the Service, and functional cookies that remember your preferences and settings.

7.2 Managing Your Cookie Preferences

You can control cookie settings through your browser preferences or through any cookie consent mechanism presented when you access the Service. Disabling certain categories of cookies may affect the functionality or performance of the platform. A full Cookie Policy detailing the types of cookies we use, their purposes, and how to manage them is available separately upon request.

CHANGES TO THIS POLICY

8.1 How We Notify You of Changes

We may update this Privacy Policy from time to time to reflect changes in our practices, the technologies we use, legal requirements, or operational needs. When we make material changes, we will notify you by posting the updated policy with a revised "Last Updated" date and, where appropriate, by sending you a direct notification via email or through the platform.

8.2 Your Continued Use

We encourage you to review this policy periodically. Your continued use of the Service after any changes take effect constitutes your acceptance of the updated terms. If you do not agree with a material change, you should discontinue use of the Service and contact us to request deletion of your data.

CONTACT US

If you have questions, concerns, or requests relating to this Privacy Policy or our data practices, please reach out to us. We are committed to addressing your inquiries promptly and transparently.

Ravn
Email: alazarsolomon.k@gmail.com

9.1 EEA and UK Users

For users in the European Economic Area or the United Kingdom, Ravn acts as the data controller for personal data processed through the Service. Where required, we have appointed a Data Protection Officer who can be reached at the email address above.

9.2 Supervisory Authority Complaints

You have the right to lodge a complaint with your local supervisory authority if you believe your data protection rights have been violated. In the Netherlands, the relevant authority is the Autoriteit Persoonsgegevens (AP). A list of EEA supervisory authorities is available on the European Data Protection Board's website.