Privacy Policy

Last updated: July 1st, 2025

Important Notice: This Privacy Policy is written in English, which serves as the authoritative version. Any translations are provided for convenience only.

This platform is designed for professional use and is not intended for individuals under the age of 18.

SCOPE AND APPLICATION

Procense, Inc. and its related entities (collectively referred to as "Procense," "we," "us," or "our") are committed to protecting your privacy and handling your personal information responsibly. This Privacy Policy explains how we collect, use, process, and protect your personal information when you interact with our websites, applications, and services.

This policy applies to:

- Our primary website at www.procense.ai
- Mobile and desktop applications
- All products and services offered by Procense (collectively, "Services")
- Any other digital platforms we operate

By using our Services, you acknowledge that you have read and understood this Privacy Policy. If you disagree with our practices described herein, please discontinue use of our Services.

Definition of Personal Information: For purposes of this policy, "Personal Information" means any information that identifies, relates to, describes, or can be linked to a specific individual, either directly or indirectly. This includes traditional identifiers like names and email addresses, as well as online identifiers, device information, and behavioral data.

Customer Data Handling: Our business customers may store and process data through our Services ("Customer Data"). We act as a processor for such data and handle it according to our service agreements with customers. This Privacy Policy does not govern our processing of Customer Data - those practices are defined in our customer contracts and data processing agreements.

Data Subject Rights: We recognize your rights regarding your personal information. If your data was submitted to us by one of our customers, please contact that customer directly to exercise your rights. If you need to contact us directly, please provide the customer name so we can route your request appropriately and respond within required timeframes.

CATEGORIES OF PERSONAL INFORMATION

We may collect the following types of personal information:

Identity and Contact Data: Full name, professional title, company affiliation, business email address, phone numbers, mailing addresses, and similar contact information.

Account and Transaction Data: Account identifiers, usernames, authentication credentials, payment information, billing records, purchase history, service usage details, support tickets, training registrations, event participation, language preferences, and communication preferences.

Professional Information: Employment details, job applications, resumes, educational background, professional experience, skills, and certifications submitted through our career portal.

Technical and Usage Data: IP addresses, browser specifications, device identifiers, operating system details, geographic location indicators, website navigation patterns, feature usage analytics, session duration, search queries, and interaction logs.

Derived Insights: Preferences, interests, and behavioral patterns we infer from the information above, such as product interests based on usage patterns or content preferences based on website interactions.

We typically collect personal information directly through your voluntary interactions with our Services. In some cases, certain information may be required to access specific features or complete particular actions (such as account creation or course enrollment).

Sensitive Information Policy: We generally avoid collecting sensitive personal information such as health data, biometric identifiers, financial account details (except for payment processing), or information about religious, political, or philosophical beliefs. When collection of such information is necessary (such as accommodation requests), we will obtain appropriate consent as required by applicable law.

INFORMATION COLLECTION METHODS

Direct Collection: We collect information directly when you:

- Register for accounts or services
- Submit support requests or feedback
- Participate in training programs, webinars, or events
- Download resources or request information
- Apply for employment opportunities
- Engage with our customer service team
- Subscribe to newsletters or communications

- Participate in surveys, contests, or promotional activities

Automatic Collection: We automatically gather certain technical information through:

- Website analytics tools and tracking technologies
- Application performance monitoring
- Security and fraud detection systems
- Customer support platform integrations

Third-Party Sources: We may supplement our records with information from:

- Business partners and resellers
- Professional networking platforms
- Marketing and lead generation services
- Public databases and directories
- Event organizers and co-sponsors

Cross-Platform Integration: Information collected across different touchpoints (website, mobile app, offline events) may be combined to provide a more comprehensive view of your interactions with Procense and improve our service delivery.

HOW WE USE YOUR INFORMATION

We process your personal information for legitimate business purposes as outlined below:

PROCESSING PURPOSE | INFORMATION CATEGORIES | LEGAL BASIS

Account management and service delivery | Identity and contact data; account and transaction data; technical and usage data | Contractual necessity and legitimate business interests in providing requested services

Customer support and technical assistance | Identity and contact data; account and transaction data; technical and usage data | Contractual necessity and legitimate business interests in maintaining customer satisfaction

Product development and service improvement | Technical and usage data; derived insights | Legitimate business interests in enhancing our offerings and user experience

Marketing and business communications | Identity and contact data; account and transaction data; derived insights | Legitimate business interests in promoting our services, with consent where required by law

Payment processing and billing | Identity and contact data; account and transaction data | Contractual necessity for completing transactions

Security monitoring and fraud prevention | All categories as needed | Legitimate business interests in protecting our systems and users

Legal compliance and dispute resolution | All categories as needed | Legal obligations and legitimate interests in protecting our rights

Employment candidate evaluation | Identity and contact data; professional information | Legitimate business interests in recruitment and human resources management

Analytics and business intelligence | Technical and usage data; derived insights | Legitimate business interests in understanding service performance and user behavior

Communication delivery and management | Identity and contact data; account and transaction data | Contractual necessity and legitimate interests in maintaining customer relationships

Event coordination and training delivery | Identity and contact data; account and transaction data | Contractual necessity and legitimate interests in providing educational services

Partnership and integration management | Identity and contact data; account and transaction data | Legitimate business interests in maintaining business relationships

Consent-Based Processing: Where we rely on consent, you may withdraw it at any time through the unsubscribe mechanisms in our communications or by contacting support@procense.ai. Withdrawal will not affect the lawfulness of processing conducted before withdrawal.

Special Considerations for Certain Jurisdictions: In the People's Republic of China (excluding Hong Kong, Macau, and Taiwan), providing information necessary for contractual performance may be processed without separate consent, or your provision of such information constitutes consent.

Data Retention: We retain personal information only as long as necessary for the purposes outlined above, to comply with legal obligations, resolve disputes, and enforce agreements. Retention periods vary based on data type, relationship nature, and legal requirements. We maintain detailed retention schedules and regularly review stored information for deletion eligibility.

Marketing Communications: If you opt into marketing communications, we maintain preference records for a reasonable period after your last interaction with us. All marketing emails include unsubscribe options.

Artificial Intelligence Usage: We employ AI technologies to enhance our operations, improve service quality, and deliver better user experiences. Our AI use complies with applicable laws and industry standards, emphasizing transparency, fairness, and data protection. We implement safeguards to protect personal information in AI systems and regularly review our practices to align with evolving standards.

INFORMATION SHARING AND DISCLOSURE

Service Providers: We engage trusted third-party providers for essential business functions including cloud hosting, payment processing, customer support, marketing automation, analytics, and security services. These providers are contractually bound to protect your information and use it only for specified purposes.

Business Partners: We may share information with authorized resellers, integration partners, and co-marketing partners when you express interest in joint offerings or services. Such sharing is governed by strict contractual protections and occurs only with appropriate safeguards.

Corporate Transactions: In connection with mergers, acquisitions, asset sales, or similar corporate events, your information may be transferred to the acquiring entity, subject to the same privacy protections outlined in this policy.

Legal Requirements: We may disclose information when required by law, legal process, or to protect the rights, safety, and security of Procense, our users, or the public. This includes cooperation with law enforcement, regulatory agencies, and judicial proceedings.

Affiliate Sharing: We may share information with current or future corporate affiliates under common control, subject to equivalent privacy protections and data handling standards.

Professional Advisors: We may share information with attorneys, accountants, auditors, and other professional service providers who assist with business operations, subject to appropriate confidentiality obligations.

Consent-Based Sharing: We may share information for other purposes with your explicit consent or as otherwise permitted by applicable law.

Data Sale Prohibition: Except for certain cookie-based advertising activities that may constitute "sales" under specific state laws, we do not sell personal information to third parties. For residents of states with specific data sale regulations, please see the relevant sections below.

TRACKING TECHNOLOGIES AND DIGITAL ANALYTICS

We utilize various technologies to collect usage information and enhance user experience:

Cookie Categories:

- **Essential Cookies:** Required for basic website functionality and cannot be disabled
- **Performance Cookies:** Help us understand how users interact with our services for improvement purposes
- **Functional Cookies:** Enable enhanced features and personalized experiences
- **Marketing Cookies:** Support targeted advertising and marketing measurement

Additional Technologies:

- **Web Beacons:** Small images that help us understand email engagement and website usage
- **Analytics SDKs:** Software components that provide insights into application performance and user behavior
- **JavaScript Tracking:** Code that monitors user interactions and technical performance

Data Collection Through Technologies: We collect information about your device, browser, location (where permitted), usage patterns, and preferences. This data helps us optimize performance, troubleshoot issues, and improve user experience.

Your Control Options: You can manage cookie preferences through your browser settings or our Cookie Preference Center (available in the website footer). Note that disabling certain cookies may impact website functionality. For analytics data, you may also configure settings within our products or block collection at the network level.

Third-Party Analytics: We partner with analytics providers like Google Analytics to better understand service usage. These providers have their own privacy policies governing their data practices.

YOUR PRIVACY RIGHTS

Depending on your location and applicable laws (including GDPR, CCPA, LGPD, PIPL, and similar regulations), you may have the following rights:

Information Access: Request details about what personal information we hold about you, how we use it, and who we share it with

Data Portability: Obtain a copy of your personal information in a structured, commonly used format

Correction and Updates: Request correction of inaccurate or incomplete personal information

Deletion Rights: Request deletion of your personal information, subject to legal and operational limitations

Processing Limitations: Request restrictions on how we use your personal information

Objection Rights: Object to processing based on legitimate interests or for direct marketing purposes

Consent Withdrawal: Withdraw previously given consent for specific processing activities

Complaint Rights: Lodge complaints with relevant data protection authorities

To Exercise Rights: Contact us at support@procense.ai with your request. We may need to verify your identity before processing requests. For California residents, you may also call our toll-free number at 1-800-PROCENSE.

Authorized Representatives: You may designate someone to make privacy requests on your behalf by providing written authorization or legal power of attorney. We will verify both your identity and the representative's authority.

Non-Discrimination: We will not discriminate against you for exercising privacy rights, including denying services, charging different prices, or providing different service quality.

Response Timeframes: We respond to verified requests within timeframes required by applicable law, typically 30-45 days depending on jurisdiction and complexity.

SECURITY MEASURES

We implement comprehensive security measures including:

Technical Safeguards: Encryption, access controls, secure data transmission, regular security assessments, and monitoring systems

Administrative Controls: Employee training, background checks, data handling policies, and incident response procedures

Physical Protections: Secure facilities, controlled access, and environmental safeguards for data centers

Payment Security: Credit card and payment information is processed by certified third-party payment processors with industry-standard security measures

Limitations: While we employ industry-standard security practices, no system is completely secure. We encourage users to protect their account credentials and report suspected security issues promptly.

User Responsibilities: Use strong, unique passwords for your Procense accounts, enable available security features, and keep your contact information current for security notifications.

REGULATORY COMPLIANCE

Procense is committed to maintaining compliance with applicable regulatory standards that govern data integrity, quality management, and electronic records in regulated industries.

21 CFR Part 11 Compliance: For customers operating under FDA regulations, our platform supports compliance with 21 CFR Part 11 requirements for electronic records and electronic signatures through:

- **Electronic Record Integrity:** Comprehensive audit trails that capture all data changes, including user identification, timestamps, and reasons for modifications
- **Electronic Signature Controls:** Multi-factor authentication, role-based access controls, and signed agreements for electronic signature authority
- **System Validation:** Documented validation processes ensuring systems perform intended functions reliably and consistently
- **Data Security:** Encrypted data storage and transmission, secure user authentication, and protection against unauthorized access or modification
- **Audit Trail Protection:** Immutable audit logs that cannot be altered or deleted without detection, with regular backup and archival procedures

Good Manufacturing Practice (GMP) Support: We provide features that support GMP compliance requirements including:

- **Data Integrity (ALCOA+):** Systems designed to ensure data is Attributable, Legible, Contemporaneous, Original, Accurate, plus Complete, Consistent, Enduring, and Available
- **Change Control:** Documented procedures for system changes with appropriate review, approval, and testing protocols
- **Personnel Training:** Comprehensive documentation capabilities for training records and qualification tracking
- **Quality Management:** Tools supporting quality assurance processes, deviation management, and corrective/preventive action (CAPA) workflows

ISO 9001 Quality Management: Our operations align with ISO 9001 principles through:

- **Quality Management System:** Documented processes for continual improvement, customer satisfaction, and systematic approach to quality
- **Risk-Based Thinking:** Proactive identification and management of risks that could affect service quality and data integrity
- **Process Approach:** Systematic management of interrelated processes to achieve consistent, predictable results
- **Customer Focus:** Regular assessment of customer requirements and satisfaction with privacy and data protection services
- **Continual Improvement:** Regular review and enhancement of privacy practices, security measures, and compliance procedures

Validation and Qualification: For regulated customers, we provide:

- **System Documentation:** Comprehensive documentation packages including functional specifications, risk assessments, and validation protocols
- **Installation Qualification (IQ):** Verification that systems are installed according to specifications
- **Operational Qualification (OQ):** Confirmation that systems operate within predetermined parameters

- **Performance Qualification (PQ):** Demonstration that systems consistently perform according to specifications under normal operating conditions
- **Periodic Review:** Regular assessment of system performance and compliance status

Regulatory Data Handling: When processing data for customers in regulated industries:

- Personal information is handled with additional safeguards appropriate for the regulatory environment
- Audit trails include enhanced detail for all data processing activities
- Data retention periods align with regulatory requirements, which may extend beyond standard business needs
- Access controls implement role-based permissions consistent with regulatory compliance needs

Customer Responsibilities: While we provide compliant infrastructure and tools, customers remain responsible for:

- Implementing appropriate procedures and controls within their organizations
- Ensuring proper user training and qualification
- Maintaining current standard operating procedures (SOPs)
- Conducting regular compliance assessments and audits

For detailed information about our regulatory compliance capabilities or to discuss specific requirements, contact support@procense.ai.

EXTERNAL LINKS AND INTEGRATIONS

Social Media Integration: Our websites may include social media features (like share buttons) that collect information about your interactions. These features are governed by the privacy policies of their respective providers.

Third-Party Links: We provide links to external websites for your convenience. We are not responsible for the privacy practices of these sites, and this policy does not apply to them.

Public Forums: Any information you post in public areas (forums, comments, reviews) may be collected and used by others. We can help remove content upon request, but cannot guarantee complete removal from all systems.

Content Responsibility: We will address reported content that violates applicable laws, but users are responsible for their own postings and interactions.

INTERNATIONAL DATA TRANSFERS

As a global organization, we may transfer personal information across borders, including to the United States and other countries that may have different data protection standards than your home country.

Transfer Safeguards: For international transfers, particularly from the EU/EEA to other countries, we implement appropriate safeguards such as:

- Standard Contractual Clauses approved by relevant authorities
- Adequacy decisions where available
- Binding corporate rules for intra-group transfers
- Additional technical and organizational measures as needed

Protection Standards: Regardless of location, we maintain consistent privacy protection standards and comply with applicable legal requirements for international data transfers.

Safeguard Information: To obtain details about specific safeguards protecting your international data transfers, contact support@procense.ai.

CHILDREN'S PRIVACY

Our Services are designed for business and professional use and are not directed toward children under 13. We do not knowingly collect personal information from children under 13 without parental consent as required by COPPA and similar laws.

Parental Rights: If you believe we have collected information about your child inappropriately, contact support@procense.ai for assistance with removal as required by law.

Teen Users: California residents under 18 may request removal of content they have posted. Email support@procense.ai with "California Minor Content Removal" in the subject line. We will make good faith efforts to remove content from public view while retaining information as necessary for legal compliance.

Minor Data Sales: We do not sell personal information of minors under 16 who are California residents without appropriate authorization.

POLICY UPDATES

We may update this Privacy Policy periodically to reflect changes in our practices, services, or legal requirements.

Notification Process: Material changes will be communicated through prominent website notices for 30 days, email notifications to registered users, and updates to the "Last Updated" date above.

Continued Use: Your continued use of our Services after policy updates constitutes acceptance of the revised terms, unless you contact us to object within the notice period.

Previous Versions: For information about previous policy versions, contact support@procense.ai.

CONTACT INFORMATION

General Privacy Inquiries: support@procense.ai

Mailing Address: Procense, Inc. [181st, 2nd St., San Francisco, CA, 94105] Attention: Privacy Team

EU Representative: [To be designated if required under GDPR Article 27]

UK Representative: [To be designated if required under UK GDPR Article 27]

For specific privacy requests, please include "Privacy Request" in your subject line and provide sufficient detail for us to process your inquiry efficiently.

CALIFORNIA PRIVACY RIGHTS SUPPLEMENT

This supplement provides additional information for California residents regarding our personal information practices under the California Consumer Privacy Act (CCPA) and related regulations.

Personal Information Sales: Under the CCPA's broad definition of "sale," our use of certain advertising and analytics cookies may constitute "sales" of the following information categories:

- Online identifiers and device information
- Internet activity and usage patterns
- Location data derived from IP addresses
- Inferred preferences and interests

Opt-Out Rights: California residents can opt out of these "sales" by:

- Using our Cookie Preference Center (website footer link)
- Configuring browser settings to reject cookies
- Contacting support@procense.ai with "Do Not Sell My Personal Information" in the subject line

Additional California Rights: Beyond the rights described above, California residents have specific rights under the CCPA including detailed disclosure requirements and specific request

procedures. All requests are subject to identity verification and may have certain limitations under law.

.