Gently Privacy Policy

Last Updated: February 2025

Introduction

At Gently ("we," "our," or "us"), we are committed to protecting your privacy and handling your data with transparency and care. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our services.

Our privacy practices are designed to comply with international standards and regulations, including:

- Service Organization Control (SOC) 2 Type 3
- ISO/IEC 27001:2022 Information Security Management
- ISO/IEC 42001:2023 Artificial Intelligence Management Systems
- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Brazil's Lei Geral de Proteção de Dados (LGPD)

Information We Collect

Personal Information

- **Account Information**: Name, email address, and other contact information when you create an account.
- **Profile Information**: Information you provide in your user profile.
- **Payment Information**: Credit card details or other payment information (processed securely through our payment processors).
- **Authentication Data**: Information used to verify your identity, including multi-factor authentication details.

- **Communication Records**: Records of your communications with our support team.

Usage Information

- **Interaction Data**: How you interact with our services, features you use, and time spent on the platform.
- **Device Information**: IP address, browser type, operating system, and device identifiers.
- **Log Data**: Information about your activities, such as pages visited and features used.
- **Performance Metrics**: Data about how our services function on your device.
- **Error Reports**: Information about any issues or crashes you experience.

AI-Related Information

- **Input Data**: Text and prompts that you provide to our AI systems.
- **Output Data**: Responses and content generated by our AI systems.
- **Training Feedback**: Feedback you provide about AI system performance (only when explicitly consented to).
- **Preference Data**: Your choices and settings for AI interactions.
- **Session Context**: Contextual information necessary to maintain coherent AI conversations.

How We Use Your Information

Service Provision and Improvement

- To provide, maintain, and improve our services
- To personalize your experience
- To respond to your requests and support needs
- To authenticate users and prevent fraud
- To process transactions and fulfill orders

Research and Development

- To develop new features and services
- To improve the accuracy and effectiveness of our AI systems
- To ensure our AI systems operate according to our ethical guidelines
- To conduct A/B testing for service optimization
- To analyze usage patterns for product development

Communications

- To send service-related communications
- To provide updates about our services
- To send marketing communications (with your consent)
- To respond to inquiries and support requests
- To send security alerts and maintenance notifications

Legal and Regulatory Compliance

- To comply with applicable laws and regulations
- To enforce our terms of service
- To protect our rights, privacy, safety, or property
- To respond to valid legal requests from public authorities
- To detect and prevent fraudulent or illegal activities

Data Isolation and Processing

Isolated Processing

All data processing occurs within our secure infrastructure. Your data is never sent to external LLM providers or third-party AI services, ensuring maximum privacy and control. We maintain complete separation between customer environments in our multi-tenant architecture.

Automated Anonymization

We automatically detect and anonymize personal identifiers before processing. This ensures that even within our systems, personal information remains protected and private. Our anonymization techniques include:

- Tokenization of personal identifiers
- Redaction of sensitive information
- Application of differential privacy techniques
- Entity recognition and masking

Data Retention

We only keep your data for as long as necessary to provide our services or comply with legal obligations. You can request deletion of your data at any time through your account settings. Our specific retention periods are:

Data Category	Retention Period	Justification
Account information	Active account period + 30 days after deletion	Service provision and continuity
Payment information	As required by financial regulations (typically 7 years)	Legal compliance
Usage logs	90 days	Security and performance monitoring
AI interaction data	30 days by default (configurable)	Service improvement and troubleshooting
Communication records	2 years	Support quality and legal compliance

Data Protection Measures

Technical Safeguards

- **Encryption**: All data is encrypted both in transit (TLS 1.3) and at rest (AES-256).
- **Access Controls**: Strict role-based access controls limit data access to authorized personnel only.
- **Monitoring**: Continuous monitoring for unauthorized access attempts and suspicious activities.
- **Network Security**: Multi-layered firewall protection, intrusion detection systems, and regular penetration testing.
- **Vulnerability Management**: Regular security scans, timely patching, and continuous security updates.
- **Authentication**: Multi-factor authentication for all administrative access and customer accounts.
- **Endpoint Protection**: Advanced threat protection on all endpoints with regular security updates.
- **Backup Systems**: Regular encrypted backups with secure off-site storage and verified recovery procedures.

Organizational Measures

- **Personnel Training**: Regular privacy and security training for all staff.
- **Data Protection Impact Assessments**: Regular assessments of data processing activities.
- **Incident Response Plan**: Comprehensive procedures to detect, report, and contain data breaches.
- **Security Clearances**: Background checks for all employees with access to sensitive systems.
- **Need-to-Know Basis**: Information access limited to what is necessary for job functions.
- **Security Governance**: Dedicated security team led by a Chief Information Security Officer (CISO).
- **Vendor Management**: Rigorous security assessment of all third-party vendors and service providers.
- **Documentation**: Comprehensive security policies and procedures aligned with ISO 27001 requirements.

AI-Specific Safeguards

- **Fairness and Bias Monitoring**: Regular testing to identify and mitigate potential biases in AI systems.
- **Explainability Mechanisms**: Tools to help understand how our AI systems reach conclusions.
- **Human Oversight**: Human review processes for critical AI operations.
- **Model Validation**: Rigorous testing protocols before deployment of new AI models.

- **Continuous Monitoring**: Real-time surveillance of AI system behavior for anomalies.
- **Ethical Guidelines**: Clear boundaries for AI operations based on our ethical principles.
- **Degradation Safeguards**: Mechanisms to detect and address model performance degradation.
- **Adversarial Defense**: Protection against manipulation attempts and prompt injection attacks.
- **Advanced Vulnerability Scanning**: We utilize an LLM Vulnerability Scanner for comprehensive security testing of our AI systems.

LLM Security Testing

We conduct customized security testing specifically tailored to our AI applications. This testing includes:

Comprehensive Vulnerability Assessments

Our AI systems undergo regular security evaluations using an advanced scanner to identify and remediate potential vulnerabilities, including:

- **PII Leaks Prevention**: Rigorous testing to prevent exposure of personally identifiable information through our AI systems.
- **Prompt Injection Defense**: Protection against unauthorized prompt manipulations that could compromise system security.
- **Jailbreaking Prevention**: Regular testing to ensure users cannot bypass our AI system's safety restrictions.
- **Excessive Agency Limitation**: Tests to verify our AI systems do not take unwanted autonomous actions.
- **Overreliance Detection**: Prevention of unwarranted reliance on incorrect input assumptions.
- **Hijacking Protection**: Safeguards against unauthorized or off-topic use of our AI systems.
- **Hallucination Minimization**: Extensive testing to reduce false or misleading information generation.
- **Competitor Endorsement Avoidance**: Testing to prevent our AI from inappropriately recommending competitor products or services.
- **Unintended Contractual Commitments**: Prevention of AI systems making promises that could be construed as contractual obligations.

Custom Security Probes

Rather than using generic scans, we employ customized security probes specifically designed for our unique AI applications and use cases, ensuring maximum effectiveness in identifying potential security issues.

Continuous Security Monitoring

We maintain ongoing surveillance of our AI systems' security posture across different models, prompts, and applications, with:

- Regular penetration testing conducted by security professionals
- Automated vulnerability scanning on a scheduled basis
- Data-driven security assessments to verify compliance with privacy and security standards

Detailed Vulnerability Reporting

All security testing produces comprehensive reports that include:

- In-depth analysis of identified vulnerabilities
- Risk assessment and prioritization
- Practical remediation recommendations
- Verification procedures to confirm successful remediation

Compliance Framework Details

SOC 2 Type 3 Implementation

Our SOC 2 Type 3 compliance ensures we meet the highest standards for security, availability, processing integrity, confidentiality, and privacy. Key aspects include:

- **External Auditing**: Annual independent audits by certified third-party assessors
- **Control Environment**: Comprehensive governance structure with board oversight
- **Risk Assessment**: Formal risk management programs with regular reviews
- **Control Activities**: Standardized procedures for critical operations
- **Information and Communication**: Clear channels for security information

- **Monitoring Activities**: Continuous evaluation of control effectiveness

ISO 27001:2022 Implementation

Our ISO 27001:2022 certification demonstrates our commitment to information security management:

- **Information Security Management System (ISMS)**: Comprehensive framework covering all aspects of information security
- **Asset Management**: Complete inventory and classification of information assets
- **Human Resources Security**: Security roles and responsibilities from pre-employment through termination
- **Physical and Environmental Security**: Controls for secure areas and equipment
- **Communications Security**: Secure information transfer policies and procedures
- **System Acquisition and Development**: Security requirements integrated throughout development lifecycle
- **Supplier Relationships**: Security requirements for external providers

Your Privacy Rights

You have the right to:

- **Access**: Request a copy of your personal data.
- **Rectification**: Correct inaccurate or incomplete data.
- **Erasure**: Request deletion of your personal data.
- **Restriction**: Limit how we process your data.
- **Object**: Object to processing based on legitimate interests.
- **Data Portability**: Receive your data in a machine-readable format.
- **Withdraw Consent**: Revoke previously given consent.
- **Non-Discrimination**: Exercise your rights without discriminatory treatment.
- **Opt-Out of Sale**: Choose not to have your personal information sold (though we do not sell your data).
- **Limit Use of Sensitive Data**: Restrict the use of sensitive personal information.

To exercise these rights, please contact us at privacy@gently.is or through your account settings. We will respond to all requests within 30 days.

Identity Verification

To protect your privacy and security, we may need to verify your identity before processing your request. We will use the least intrusive means possible, typically using information already in our systems.

Authorized Agents

You may designate an authorized agent to make requests on your behalf. We will require verification of both your identity and the agent's authority to act for you.

International Data Transfers

We process data within secure data centers located in the European Union and the United States. When transferring data internationally, we ensure appropriate safeguards are in place, including:

- Standard Contractual Clauses
- Data Processing Agreements
- Security assessments of processors
- Binding Corporate Rules for intragroup transfers
- Regional data residency options for customers with specific compliance needs

Regional Compliance

We maintain specific measures to comply with regional data protection laws:

European Economic Area (EEA)

- Implementation of GDPR requirements

- Data Processing Impact Assessments for high-risk processing
- EU Representative appointment
- Regular compliance reviews

United States

- Compliance with state-specific laws (CCPA, CPRA, VCDPA, etc.)
- Privacy notice requirements
- Opt-out mechanisms
- Consumer rights processes

Asia-Pacific

- Compliance with APPI (Japan), PIPL (China), PDPA (Singapore), and other relevant laws
- Data localization where required
- Specific consent mechanisms
- Regional representatives where required

Security Incident Management

Incident Response

We maintain a comprehensive incident response plan that includes:

- **Detection**: Advanced monitoring systems to identify potential incidents
- **Analysis**: Rapid assessment of security events to determine severity and impact
- **Containment**: Immediate actions to limit incident impact
- **Eradication**: Complete removal of incident causes

- **Recovery**: Restoration of affected systems to normal operation
- **Post-Incident Analysis**: Thorough review to prevent recurrence

Breach Notification

In the event of a data breach affecting your personal information, we will:

- Notify affected individuals without undue delay, typically within 72 hours of discovery
- Provide details about the breach, including what information was affected
- Explain steps we've taken to mitigate harm
- Offer recommendations for personal protection measures
- Notify relevant regulatory authorities as required by law

Cookie Policy

We use cookies and similar technologies to:

- Maintain your session
- Remember your preferences
- Analyze usage patterns
- Improve our services

We primarily use essential cookies that are necessary for our services to function properly. You can control non-essential cookies through your browser settings or our cookie preference center.

Cookie Types

- **Essential Cookies**: Required for basic functionality
- **Functional Cookies**: Enhance user experience by remembering preferences

- **Analytical Cookies**: Help us understand how visitors interact with our services
- **Marketing Cookies**: Used to deliver relevant advertisements (only with explicit consent)

Cookie Management

You can manage your cookie preferences through:

- Our cookie consent banner
- Your account privacy settings
- Your browser's cookie settings
- Industry opt-out tools like the Digital Advertising Alliance opt-out platform

AI Governance

In accordance with ISO/IEC 42001:2023, we have implemented a comprehensive AI management system that includes:

Risk Assessment

- Regular assessments of AI system risks
- Continuous monitoring of model behavior
- Proactive identification of potential issues
- Formal risk categorization and mitigation strategies
- Regular third-party audits of AI systems

Accountability

- Clear assignment of responsibilities for AI oversight
- Documentation of AI system development and operations
- Regular audits of AI systems

- Designated AI Ethics Committee with independent members
- Escalation pathways for AI-related concerns

Transparency

- Clear information about AI use in our services
- Explanations of how AI systems make decisions when possible
- Documentation of AI system capabilities and limitations
- Disclosure of automated decision-making processes
- Regular transparency reports on AI usage

AI Ethics Framework

Our AI operations are guided by the following principles:

- **Human-Centered Design**: AI systems that augment human capabilities rather than replace human judgment
- **Fairness and Non-Discrimination**: Systems designed to treat all users equitably
- **Safety and Reliability**: Rigorous testing to ensure AI systems function as intended
- **Privacy by Design**: Privacy considerations integrated from the earliest design stages
- **Sustainability**: Consideration of environmental impacts in AI development and deployment

AI Lifecycle Management

We manage AI systems throughout their entire lifecycle:

- **Design and Development**: Ethical considerations integrated from conception
- **Testing and Validation**: Comprehensive evaluation before deployment
- **Deployment**: Controlled rollout with monitoring systems
- **Operation**: Continuous performance and fairness monitoring

- **Retirement**: Responsible decommissioning of outdated models

Subprocessors and Service Providers

We carefully select vendors and service providers who maintain high security and privacy standards. All third parties who process data on our behalf are bound by Data Processing Agreements that require them to:

- Process data only according to our instructions
- Implement appropriate security measures
- Assist with data subject rights requests
- Support our compliance obligations
- Allow for audits and inspections

Current Subprocessors

Service Provider	Processing Purpose	Location	Data Protection Framework
Amazon Web Services	Cloud infrastructure	Global	SOC 2, ISO 27001, GDPR
Paddle	Payment processing	Global	PCI DSS, SOC 2, GDPR
Zendesk	Customer support	Global	SOC 2, ISO 27001, GDPR
Datadog	Monitoring and logging	EU, US	SOC 2, GDPR
Cloudflare	Content delivery and security	Global	SOC 2, ISO 27001, GDPR
Google Drive	Document storage and collaboration	Global	SOC 2, ISO 27001, GDPR
Salesforce	Customer relationship management	Global	SOC 2, ISO 27001, GDPR
Microsoft SharePoint	Document management and collaboration	Global	SOC 2, ISO 27001, GDPR

Service Provider	Processing Purpose	Location	Data Protection Framework
Jira	Project and issue tracking	Global	SOC 2, ISO 27001, GDPR
Confluence	Team collaboration and knowledge sharing	Global	SOC 2, ISO 27001, GDPR

Changes to This Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our practices or for other operational, legal, or regulatory reasons. We will notify you of any material changes by:

- Posting the updated policy on our website
- Sending an email to the address associated with your account
- Displaying a notice within our services

Version History

We maintain a complete history of our privacy policy versions, available upon request. Major policy changes are documented with details about what changed and why.

Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Privacy Team
Email: privacy@gently.is

For urgent privacy matters, please contact our Data Protection Officer at dpo@gently.is.

Response Timeframes

We are committed to addressing your privacy concerns promptly:

- General inquiries: 2 business days
- Data subject rights requests: 30 calendar days (may be extended by an additional 60 days for complex requests)
- Urgent security concerns: 24 hours

Legal Basis for Processing

For users in the European Economic Area (EEA), we process your personal data based on the following legal grounds:

- Performance of a contract when providing our services
- Legitimate interests for improving our services
- Compliance with legal obligations
- Your consent, where required

Legitimate Interests Assessment

When relying on legitimate interests, we conduct balancing tests to ensure our interests do not override your fundamental rights and freedoms. Key legitimate interests include:

- Service improvement and development
- Fraud prevention and security
- Analytics to understand user needs
- Business continuity and service optimization

Children's Privacy

Our services are not directed to children under 16. We do not knowingly collect personal information from children under 16. If we learn that we have collected personal information from a child under 16, we will promptly delete that information.

Age Verification

Where appropriate, we implement age verification measures to prevent collection of data from minors. If you believe we have inadvertently collected information from a child, please contact us immediately.

Data Protection Authority

You have the right to lodge a complaint with a supervisory authority if you believe our processing of your personal data violates applicable law.

EU Supervisory Authorities

EU residents can find their national data protection authority through the European Data Protection Board website: https://edpb.europa.eu/

US State Authorities

US residents can contact their state attorney general's office for privacy concerns.

This Privacy Policy was last updated on February 2025.