

PRIVACY POLICY

Data Controller: Faciliter AI, a Société par Actions Simplifiée Unipersonnelle (SASU)

Registered Office: 100 chemin de Mireille, 13300 Salon-de-Provence, France

VAT No: FR14938793775

Contact: contact@faciliter.ai

Data Protection Officer: dpo@faciliter.ai

Version: 1.0

Effective Date: February 1, 2026

1. INTRODUCTION

Faciliter AI ("we", "us", "our") is committed to protecting your privacy and personal data. This Privacy Policy explains how we collect, use, store, and protect your personal information when you use the MyFAQ platform and related services (the "Service").

This policy applies to all users of the Service, including organization administrators, invited team members, and visitors to our website.

2. DATA WE COLLECT

2.1 Account Information

When you register or are invited to use the Service, we collect:

- Name (first name, last name)
- Email address
- Company name and website
- Country of residence
- Language preferences
- Job title (optional)

2.2 Usage Data

We automatically collect information about how you use the Service:

- Log data (IP address, browser type, device information)
- Feature usage and interaction patterns
- Query volumes and service performance metrics
- Error logs for debugging and improvement

2.3 Content Data

We process content you upload to the Service, including:

- Documents (RFPs, PDFs, Excel files)
- Question and answer pairs
- Knowledge base content

2.4 Billing and Tax Information

Where needed to provide a paid subscription, issue invoices or meet tax and accounting obligations, we collect:

- Billing contact name and email address

- Company legal name, billing address and country
- VAT, tax or other business identification number
- Purchase-order, invoice and payment-status information

2.5 Consent Records

We maintain records of your consent for legal compliance:

- Terms of Service acceptance timestamp
- Privacy Policy acceptance timestamp
- Acceptable Use Policy acceptance timestamp
- Policy versions accepted

3. HOW WE USE YOUR DATA

3.1 Service Provision (Legal basis: Contract performance)

- Providing and maintaining the Service
- Processing your requests and queries
- Managing your account and subscription
- Sending service-related communications

3.2 Service Improvement (Legal basis: Legitimate interest)

- Analyzing usage patterns to improve features
- Developing new functionality
- Troubleshooting technical issues
- Optimizing AI search and retrieval algorithms

3.3 Legal Compliance (Legal basis: Legal obligation)

- Complying with applicable laws and regulations
- Responding to lawful requests from authorities
- Maintaining audit trails for compliance purposes
- Issuing invoices, calculating and reporting applicable taxes, and retaining accounting records

3.4 Marketing (Legal basis: Consent)

- Sending newsletters and product updates (with your consent)
- Providing information about new features or services

4. DATA SHARING

4.1 Service Providers

We share data with trusted service providers who assist in operating the Service:

Selected Data Region: The Customer selects either the EU/EEA or North America data region during registration. That selection determines where Customer Content and primary Service data are hosted and processed, subject to the provider and transfer disclosures below.

- **Cloud Infrastructure:** OVH and other vetted cloud and infrastructure providers, in the EU/EEA, the United States or other locations as needed
- **Payment Processing:** Stripe (PCI-DSS compliant)
- **AI Processing:** Google (Gemini), Mistral, OVH-hosted models and other vetted AI providers, including providers in the United States where needed - contractually restricted from using your data to train their models
- **Email Services:** For transactional and marketing emails

We may add, replace or use additional providers where needed to operate, secure, support or improve the Service, subject to appropriate due diligence and contractual data-protection obligations. Providers may process data in the EU/EEA, the United States or other countries. For transfers of personal data outside the EEA, we use a legally valid transfer mechanism, such as an adequacy decision (including the EU-US Data Privacy Framework where applicable), European Commission Standard Contractual Clauses with supplementary measures where required, or another mechanism permitted by applicable data-protection law.

4.2 Legal Requirements

We may disclose data when required by law, legal process, or to protect our rights and safety.

4.3 No Sale of Data

We do NOT sell your personal data to third parties.

5. AI AND YOUR DATA

5.1 No Training Covenant

We covenant that your content will NOT be used to train, fine-tune, or improve third-party Foundation Models (such as GPT-4, Claude, Gemini) shared with other customers or the public.

5.2 Processing for Service Delivery

Your content is processed solely to generate responses and provide the Service to you. AI providers are contractually bound to process data only for our specified purposes.

5.3 Anonymized Improvements

We may use anonymized, aggregated data to improve our internal algorithms (RAG retrieval, search optimization) in ways that cannot identify you or your content.

5.4 Google API Services User Data Policy

When you choose to connect your Google Drive to the Service, our access, use, transfer, protection, and retention of Google user data is governed by the following disclosures:

- **Data Access:** We access your Google account profile information (specifically email address and basic profile info) to authenticate the connection. We also access Google Drive files and folders (metadata like file names, IDs, sizes, and file content) that you explicitly select using our file picker integration.
- **Data Use:** We use your Google Drive files exclusively to import them into your isolated knowledge base and use our AI agent to answer your questions based on those documents. We do not use the data for any other purpose.
- **Data Transfer:** We do not transfer or sell Google user data to any third parties, including data brokers or advertisers. Google user data is processed solely on our secure EU servers. To generate AI responses for you, the content of selected documents is sent to our AI API providers (such as Google Gemini, Mistral, or OVH-hosted models) which are contractually bound to NOT retain or use your data to train their public models.
- **Data Protection:** Google user data is protected using high-level industry security standards, including encryption in transit (TLS 1.3) and at rest (AES-256), strict tenant isolation, and regular security audits.
- **Data Retention & Deletion:** We store imported Google Drive file content only as long as your account is active or until you delete the document from the knowledge base. If you delete a document, it is immediately removed from active systems and permanently purged from backups within 90 days. If you disconnect your Google account, all associated tokens are deleted immediately.
- **Limited Use Compliance:** MyFAQ's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Specifically: We do not use Workspace data (such as Google Drive files) to develop, improve, or train AI/ML models (including large language models). We do not transfer Workspace data to third-party services that use that data to train their AI/ML models.

6. DATA RETENTION

6.1 Active Accounts

We retain your data for as long as your account is active and as needed to provide the Service.

6.2 After Termination

Upon account termination:

- You have 30 days to export your data
- After 30 days, we delete your content from active systems
- Backup copies may be retained for up to 90 days
- Anonymized analytics may be retained indefinitely

6.3 Legal Requirements

Some data may be retained longer to comply with legal obligations (e.g., billing records for tax purposes).

7. DATA SECURITY

We implement appropriate technical and organizational measures:

- Encryption in transit (TLS 1.3) and at rest (AES-256)
- Access controls and authentication
- Regular security assessments
- Employee training and confidentiality agreements
- Incident response procedures

8. YOUR RIGHTS (GDPR)

As a data subject under GDPR, you have the right to:

- **Access:** Request a copy of your personal data
- **Rectification:** Correct inaccurate data
- **Erasure:** Request deletion of your data ("right to be forgotten")
- **Portability:** Export your data in a machine-readable format
- **Restriction:** Limit how we process your data
- **Objection:** Object to processing based on legitimate interest
- **Withdraw Consent:** Where processing is based on consent

To exercise these rights, contact us at dpo@faciliter.ai.

9. INTERNATIONAL TRANSFERS

9.1 Selected Data Region

At registration, the Customer selects either the EU/EEA or North America data region. Customer Content and primary Service data are primarily hosted and processed in the selected region.

9.2 Third-Party Transfers

Service providers may process data in the EU/EEA, the United States or other countries where needed to operate, secure, support or improve the Service. When personal data is transferred outside the selected region or, where applicable, outside the EEA, we use safeguards required by applicable data-protection law, such as an adequacy decision (including the EU-US Data Privacy Framework where applicable), Standard Contractual Clauses with supplementary measures where required, or another permitted transfer mechanism.

10. COOKIES

We use essential cookies for Service functionality and optional analytics cookies with your consent. See our Cookie Policy for details.

11. CHILDREN'S PRIVACY

The Service is not intended for individuals under 18 years of age. We do not knowingly collect data from children.

12. CHANGES TO THIS POLICY

We may update this Privacy Policy periodically. Material changes will be notified via email or through the Service. Continued use after notification constitutes acceptance.

13. SUPERVISORY AUTHORITY

You have the right to lodge a complaint with your local data protection authority. For France, this is the Commission Nationale de l'Informatique et des Libertés (CNIL).

14. CONTACT US

For privacy-related inquiries:

- **Email:** dpo@faciliter.ai
- **Address:** Faciliter AI, 100 chemin de Mireille, 13300 Salon-de-Provence, France