

Privacy Policy

Effective Date: 01.01.2026

Last updated: 13.02.2026

This Privacy Policy explains how **DataMinder sp. z o.o.** ("DataMinder", "we", "our", or "us") collects, uses, stores, discloses, and protects personal data when you access our website <https://dataminder.ai/>, applications, and related services (collectively, the "Services").

This Policy is designed to comply with:

- Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)
 - The Polish Act on Personal Data Protection
 - UK GDPR
 - California Consumer Privacy Act (CCPA/CPRA)
 - Other applicable international data-protection laws
-

1. Data Controller

The controller of your personal data is:

DataMinder sp. z o.o.

Registered in Poland

Address: Lipnowska 207, 09-400 Maszewo Duże, Poland

Email: contact@dataminder.ai

If required by law, we may appoint a Data Protection Officer (DPO). You will be informed accordingly.

2. Categories of Personal Data We Collect

2.1 Data You Provide Directly

- Identification data (name, surname)
- Contact data (email address, institutional affiliation)

- Account credentials (encrypted password)
- Billing and payment-related data (processed via payment providers)
- Communication content (support messages, feedback)
- Marketing preferences (if consent provided)

2.2 Data Generated Through Use of the Services

- Usage data (selected analyses, modules used, feature interaction logs)
- AI interaction data, including prompts, generated outputs, chat history, and project-related content
- Uploaded datasets and files
- Generated reports (e.g., HTML, PDF, DOCX)
- Technical logs for debugging, monitoring, and performance optimization
- Preferences and configuration settings

2.3 Technical and Device Data

- IP address
- Browser type and version
- Operating system
- Device identifiers
- Approximate geolocation (country / region level)

2.4 Cookies and Similar Technologies

Details are described in Section 10.

3. Special Categories of Personal Data

DataMinder does not intentionally collect special categories of personal data (e.g., health data, biometric data).

If users upload datasets containing personal or sensitive data:

- The User / Institution acts as the Data Controller
- DataMinder acts solely as a Data Processor under Article 28 GDPR
- Users are responsible for ensuring lawful processing, appropriate legal basis, and required anonymization or pseudonymization

DataMinder does not verify the legality of uploaded datasets.

4. Legal Bases for Processing (GDPR Article 6)

We process personal data based on:

- Consent (Article 6(1)(a)) – newsletters, optional analytics, cookies
- Contract performance (Article 6(1)(b)) – account creation, service delivery
- Legal obligation (Article 6(1)(c)) – accounting, tax, regulatory duties
- Legitimate interests (Article 6(1)(f)) – service improvement, security, fraud prevention, infrastructure protection

You may withdraw consent at any time without affecting prior lawful processing.

5. Purposes of Processing

We process personal data to:

- Provide and operate the Services
- Enable statistical analysis and AI-assisted insights
- Store user projects and analysis history
- Manage user accounts and subscriptions
- Process payments and invoices
- Communicate service-related information
- Improve functionality, usability, and security
- Detect abuse, fraud, or misuse of the platform
- Comply with legal obligations

We do not use personal data for automated decision-making producing legal or similarly significant effects.

6. AI and Automated Processing Transparency

DataMinder uses AI-assisted systems to:

- Recommend analytical methods
- Generate reports and structured explanations
- Assist with hypothesis formulation and statistical interpretation

AI outputs are supportive and advisory only and do not replace human judgment. Final decisions remain the user's responsibility.

AI processing is performed through infrastructure provided by **Microsoft (Azure AI Foundry)**.

DataMinder ensures that:

- User data is not used to train general or third-party AI models
- AI processing occurs within secured infrastructure
- Outputs are generated solely for the requesting user

AI components operate under contractual data-protection safeguards.

7. Data Sharing and Recipients

We do not sell personal data.

7.1 Processors

Data may be processed by trusted service providers acting as sub-processors under Data Processing Agreements (DPAs).

As of the effective date, these include:

- **Amazon Web Services (AWS)** – cloud infrastructure and database hosting
- **Microsoft (Azure AI Foundry)** – AI processing infrastructure
- **Stripe, Inc.** – payment processing and subscription management
- **Google LLC** – email infrastructure and corporate tools
- **Supabase (legacy use)** – database services (being phased out)
- **Cloudflare, Inc.** – DNS and network protection
- **GitHub, Inc.** – code repository hosting

A current list of sub-processors may be provided upon request.

7.2 Legal and Business Transfers

Data may be disclosed:

- To public authorities where legally required
 - In connection with mergers, acquisitions, or asset transfers
-

8. International Data Transfers

Some service providers (e.g., Microsoft, Stripe, Google) may process data outside the European Economic Area (EEA).

Where international transfers occur, DataMinder ensures appropriate safeguards, including:

- Standard Contractual Clauses (SCCs)
 - Adequacy decisions (e.g., EU-US Data Privacy Framework)
 - Additional technical and organizational measures
-

9. Data Retention

Personal data is retained only as long as necessary:

- Account data – for the duration of the account
- Billing data – as required by tax and accounting laws
- AI interaction logs – limited retention for service continuity and debugging
- Research datasets – retained only as long as necessary to provide the Services

Unless otherwise agreed, research datasets are deleted or irreversibly anonymized within 30 days after account termination, unless legal obligations require longer retention.

10. Cookies and Tracking

We use:

- Necessary cookies (essential for platform operation)
- Functional cookies
- Analytical cookies (consent-based)

Users can manage cookie preferences through consent tools or browser settings.

11. Your Rights

GDPR / UK GDPR

You have the right to:

- Access
- Rectification
- Erasure
- Restriction of processing
- Data portability
- Objection
- Withdraw consent
- Lodge a complaint with a supervisory authority

CCPA / CPRA (California)

You have the right to:

- Know what personal data is collected
- Request deletion
- Opt-out of data sale (we do not sell data)
- Non-discrimination

Requests may be sent to:
privacy@dataminder.ai

12. Data Security

We implement appropriate technical and organizational measures, including:

- Encryption in transit (TLS)
- Secure cloud infrastructure
- Role-based access control
- Monitoring and incident detection
- Periodic security reviews

No system is fully secure. Users share data at their own risk.

13. Third-Party Links

Our Services may contain links to third-party websites. We are not responsible for their privacy practices.

14. Changes to This Policy

We may update this Policy from time to time.

Material changes will be communicated via the Services or email.

Continued use of the Services constitutes acceptance of the updated Policy.

15. Contact

For privacy-related questions:

DataMinder sp. z o.o.

Lipnowska 207, 09-400 Maszewo Duże, Poland

Email: contact@dataminder.ai