DATAMINDER PRIVACY POLICY

Version: DM-PP-310826-EN | Effective date: 31 August 2026

1. Key information

This Policy explains how DataMinder sp. z o.o. processes personal data of persons visiting DataMinder websites, creating an account, using the application, making payments, contacting us, subscribing to a newsletter or waiting list, participating in tests or recorded meetings and using DataMinder profiles in social media.

Topic	Key information
Controller	DataMinder sp. z o.o., ul. Lipnowska 207, 09-400 Maszewo Duże, Poland.
Contact	contact@dataminder.ai
Main purposes	Providing and securing the Service, account administration, payments, contact and support, AI features, meeting recording, analytics and marketing - depending on the user's choices.
Customer data	For personal data contained in customer datasets, DataMinder generally acts as a Processor and the customer acts as the Controller.
Rights	Access, rectification, erasure, restriction, portability, objection, withdrawal of consent and the right to lodge a complaint with the President of the Polish Data Protection Authority (UODO), depending on the legal basis and circumstances.

2. Controller and contact

The controller of personal data processed for DataMinder's own purposes is DataMinder sp. z o.o., with its registered office at ul. Lipnowska 207, 09-400 Maszewo Duże, Poland, entered in the Register of Entrepreneurs of the National Court Register under KRS 0001152130, NIP 7743295226, REGON 540761152 ('DataMinder', 'we', 'us').

For matters relating to privacy, exercise of rights or data security, please contact us at contact@dataminder.ai. We may ask for information necessary to confirm your identity if this is necessary for the secure handling of your request.

3. Scope of this Policy and DataMinder's roles

3.1. DataMinder as Controller

We act as the Controller where we independently determine the purposes and means of processing, including for account administration, authentication, payments and credits, security and diagnostics, contact and support, service communications, newsletters, analytics, marketing, tester recruitment, meeting recording and transcription, and the handling of rights and legal claims.

3.2. DataMinder as a Processor

If a customer uploads a dataset containing other individuals' personal data and determines the purpose of the analysis, the customer remains the Controller of that data and DataMinder generally processes it as a Processor on the customer's documented instructions. This processing is governed by the applicable Data Processing Agreement (DPA). Individuals whose data is included in a customer dataset should contact that customer first.

DataMinder may nevertheless act as an independent Controller for separate information generated while providing the Service, such as billing data, security records, logs required to protect the system, or information needed to establish, exercise or defend legal claims. DataMinder's role is assessed separately for each processing purpose.

4. What data we process

Category	Examples
Account and identification	Name, email address, account ID, settings, authentication data or Google OAuth token.
Projects and analyses	Files, datasets, schemas, field names, sample values, hypotheses, analysis settings, results, charts, reports and notebooks.
AI features	Instructions and messages, conversation history, attachments, dataset statistics, analysis results, responses, reports, errors and execution metadata.
Payments and billing	Customer and transaction data, country or region, payment status and Stripe identifiers. Card details are provided directly to Stripe.
Contact and support	Contact details, correspondence and attachments, and information about the account, project, device, browser and errors.
Technical and security data	IP address, timestamps, session, device and request identifiers, logs, diagnostic information and unusual-activity indicators.
Analytics and marketing	Online identifiers, device and browser data, approximate location, page views, clicks, navigation, interactions and conversions – only after the required consent.
Social media	Profile name, public profile information, reactions, comments and messages sent to DataMinder profiles.

Category	Examples
Meeting recordings	Voice, image where recorded, statements, transcripts, notes, summaries and metadata - only after the required consent.

The scope of the data depends on how the Service is used and on the content provided by the user. Before uploading a dataset, the user must remove unnecessary data, direct identifiers and information that would enable DataMinder to identify an individual directly and unambiguously. If data is pseudonymised, the re-identification key must be kept separately by the user and must not be provided to DataMinder. Special categories of personal data, data relating to criminal convictions and offences, and children's data may be processed only after data minimisation and at least pseudonymisation, without providing the re-identification key, where the user has an appropriate legal basis and has implemented safeguards proportionate to the risk. Properly anonymised data is not personal data; pseudonymised data remains subject to the GDPR.

5. Purposes and legal bases

The purposes, legal bases, categories of data, retention criteria and data sources are described in Appendix 2 - Purposes of Personal Data Processing, which forms part of this Policy. In summary:

Purpose	Legal basis
Account, authentication, projects, analyses, Credits and service communications	Article 6(1)(b) GDPR - entering into and performing the agreement.
Payments, accounting, tax, complaints and data subject rights	Article 6(1)(b) or (c) GDPR - performance of the agreement and compliance with legal obligations; where appropriate, Article 6(1)(f) GDPR.
Security, diagnostics, fraud prevention, support and legal claims	Article 6(1)(f) GDPR - DataMinder's and users' legitimate interests; for security obligations, also Article 6(1)(c) GDPR.
Newsletter, waiting list, meeting recording, analytics and advertising	Article 6(1)(a) GDPR - consent; for communications and terminal-equipment technologies, also Articles 398-399 of the Polish Electronic Communications Law.
Personal data in customer datasets	Article 28 GDPR and the customer's documented instructions. The customer, as Controller, determines the basis under Article 6 and, where applicable, Article 9 GDPR.

Where we rely on legitimate interests, we assess whether the processing is necessary and consider its impact on individuals' rights. You may object on grounds relating to your particular situation. An objection to processing for direct marketing purposes is unconditional.

6. Is data mandatory

Providing data required for registration, payment or a particular feature is voluntary, but necessary to enter into or perform the agreement or to carry out the requested action. Without data marked as required, we may be unable to create an account, process a payment, perform an analysis or respond to a request.

Providing data for newsletters, the waiting list, analytics, advertising or meeting recording is voluntary. Refusing or withdrawing consent does not affect access to the core Service features that do not require that consent.

7. Sources of personal data

- directly from you - when you register, use the Service, make a payment, contact us, subscribe to a newsletter or attend a meeting;
- from a customer or a person acting on the customer's behalf - where the data is included in an uploaded dataset;
- automatically from your device, browser, the application and infrastructure - for technical, security and activity data;
- from providers of authentication, payments, communications, meeting recording and transcription, analytics, advertising and social media - to the extent resulting from the feature and settings used;
- from outputs generated by DataMinder - such as analyses, reports, AI responses and usage-accounting information.

8. Data recipients and external tools

We may disclose data to entities supporting the operation of DataMinder, only to the extent necessary for a given purpose. These include cloud infrastructure providers, AI systems, mail and authentication, payments, content hosting, meeting recording and transcription, analytics, usability research, advertising, and social networking.

A public list of tools used, contractual entities, purposes of use and supplier documents can be found in Appendix 1 – List of external tools. The list includes, among others, AWS, Microsoft Foundry / Azure OpenAI, Google Workspace and Google OAuth, Google Analytics 4, Stripe, Sanity, Hotjar, Meta Pixel, Fireflies.ai and DataMinder profiles in LinkedIn, Facebook and Instagram.

The data may also be made available to authorized employees and associates, legal and accounting advisors, banks, payment operators and public authorities if it is required by law or is necessary to establish, pursue or defend claims.

9. Transfers outside the European Economic Area

Because we use certain providers, including AWS, Google, Meta, LinkedIn, Sanity, Hotjar, Stripe, Microsoft and Fireflies.ai, personal data may be transferred to, or accessed from, countries outside the European Economic Area. Fireflies.ai stores and processes data in the United States by default.

Transfers rely on an appropriate mechanism under Chapter V GDPR, including an adequacy decision, the EU-US Data Privacy Framework for a covered certified entity, or Standard Contractual Clauses together with supplementary safeguards where required.

The mechanisms identified by providers include the EU-US Data Privacy Framework for covered certified entities in the United States and the Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914 where an adequacy decision does not apply. Provider-specific transfer documents and conditions are listed in Appendix 1. On request, we will provide information about the safeguards used or explain where a copy can be obtained.

10. Data retention

Account, project, notebook, dataset and report data remains in an active account without a predetermined expiry date until deleted by the user, the account is deleted, or the agreement ends in circumstances requiring deletion. Deleting a project removes the information and results associated with that project, but does not delete a dataset or source file stored separately in the account; the dataset or file is deleted on a separate user instruction or when the account is deleted. Account deletion triggers removal of all related data and artefacts from active systems, caches, queues and provider-held copies within 30 days. Automated RDS backups are overwritten on a retention cycle of no more than 35 days, while application and database logs are retained for one month and LLM traces for no more than 90 days. Until deletion, backups are isolated from ordinary processing and may be used only to restore the system following a failure, loss or corruption of data, or for necessary security activities. Data required by law or needed to establish, exercise or defend legal claims may be retained longer, but only to the extent necessary. Fireflies.ai meeting recordings, transcripts, summaries and notes are retained for three months from the meeting date and may be deleted earlier following withdrawal of consent where no other legal basis requires continued retention.

Data	Current retention period or criterion
ECS CloudWatch logs	30 days.
Accounting records	Generally five years, calculated in accordance with Article 74 of the Polish Accounting Act.
Tax records	Until the relevant tax liability becomes time-barred, generally five years from the end of the calendar year in which the payment deadline expired.
Data processed on the basis of consent	Until consent is withdrawn or the relevant purpose ends. Evidence of consent may be retained for the period necessary to demonstrate compliance and defend legal claims.
Lambda and database logs	One month.
LLM traces in self-hosted Langfuse	90 days. Following account deletion, this is the outer limit for deletion of associated logs and traces.
Other data	Detailed retention criteria are set out in Appendix 2.

Data	Current retention period or criterion
Meeting recordings, transcripts and notes	Three months from the meeting date; earlier following withdrawal of consent where no other legal basis requires continued retention.

11. Cookies, device storage, analytics and marketing

11.1. Necessary technologies and preferences

DataMinder uses technologies necessary for authentication, security and remembering privacy choices. Identified first-party technologies include an authentication cookie (30 days), an interface-settings cookie (7 days), a language-preference cookie (1 year), and local storage for consent choices and bookmarks. Some local-storage entries do not have a technically configured expiry date.

11.2. Analytics, usability testing and advertising

After obtaining the appropriate consent, we use Google Analytics 4 to measure use of the Service, Hotjar to study usability, and Meta Pixel to measure campaigns, conversions and advertising. These tools remain disabled before consent is given, after consent is refused and after consent is withdrawn, and do not collect data during those periods. Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn. Provider information is available in Appendix 1.

The legal basis for processing personal data is consent under Article 6(1)(a) GDPR. Storing information on, or accessing information from, a user's terminal equipment also requires consent under Article 399 of the Polish Electronic Communications Law. Consent may be withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal.

12. Newsletter and marketing communication

We send newsletters and other marketing communications on the basis of voluntary consent under Article 6(1)(a) GDPR and the consent required by Article 398 of the Polish Electronic Communications Law. You may unsubscribe at any time by using the unsubscribe link in the relevant message or by emailing contact@dataminder.ai.

After you unsubscribe, we may retain the minimum information needed on a suppression list to respect your choice, together with evidence of consent and its withdrawal for as long as necessary to demonstrate compliance and defend legal claims.

13. Recording, transcribing and meeting notes

Once the required consent has been obtained from meeting participants, we may use Fireflies.ai to record a meeting and prepare a transcript, summary and notes. The data may include participant names or identifiers, email addresses, calendar data, voice, image where recorded, the content of

statements and meeting metadata. Refusing a recording does not restrict access to DataMinder's core features.

Meeting materials are retained for three months. If a meeting involves Customer Personal Data, DataMinder processes it on the customer's documented instructions and Fireflies.ai acts as a Subprocessor. Fireflies.ai stores and processes data in the United States by default. Appendix 1 contains information about transfer mechanisms and provider documents.

14. Artificial intelligence and automated decisions

DataMinder uses Microsoft Foundry / Azure OpenAI for generative features that support hypothesis formulation, explanation and presentation of results, and the creation of reports and supporting content. Statistical calculations are performed by a separate deterministic component. Further information is provided in Appendix 3 – Information on the Use of Artificial Intelligence.

Users are informed when they interact with an AI feature. AI outputs are supportive, may contain errors and should be verified. Based on the current Service design, DataMinder does not make decisions about users based solely on automated processing that produce legal effects or similarly significantly affect them within the meaning of Article 22 GDPR.

15. Data security

We apply technical and organisational measures appropriate to the nature of the data and the risk, including access controls, encryption in transit, infrastructure safeguards, backups, event logging and restrictions on personnel access. We regularly assess whether the safeguards should be updated.

No method of transmission or storage can guarantee absolute security. If you suspect a breach or unauthorised access to your account, contact us immediately at contact@dataminder.ai.

16. Rights of persons

Depending on the legal basis and circumstances, you may have the following rights:

- access to your personal data and a copy of it;
- rectification of inaccurate data or completion of incomplete data;
- erasure of personal data;
- restriction of processing;
- data portability where processing is automated and based on consent or a contract;
- objection to processing based on legitimate interests, including an unconditional right to object to direct marketing;
- withdrawal of consent at any time, without affecting the lawfulness of processing carried out before withdrawal;
- the right not to be subject to a decision based solely on automated processing in the circumstances described in Article 22 GDPR.

To exercise your rights, email contact@dataminder.ai. We will respond without undue delay and generally within one month. That period may be extended by two further months where necessary because of the complexity or number of requests; we will inform you of the extension and explain the reasons.

You also have the right to lodge a complaint with the President of the Polish Data Protection Authority (UODO). Current information on how to submit a complaint is available at https://uodo.gov.pl.

17. Children's data

The DataMinder Service is not intended for minors, and minors are not permitted to create accounts. If you believe that a minor has provided personal data to us, contact us at contact@dataminder.ai.

18. Social media profiles

We maintain DataMinder profiles on LinkedIn, Facebook and Instagram. When you comment, react or send a message, we process information visible in your profile and the content of the interaction to communicate with you and operate the profile, relying on our legitimate interests or, where the contact concerns an agreement, to take steps at your request or perform that agreement.

The platform operator processes data under its own terms and may in some cases act with us as a joint controller for specified statistics or advertising activities. Please also consult the privacy policy of the relevant platform identified in Appendix 1.

19. Policy changes

We may update this Policy when the law, Service, providers, processing purposes or use of data changes. The new version will be published with its effective date. If a change materially affects Users' rights or the manner of processing, we will provide additional information appropriate to the nature of that change.

20. Appendices forming part of this Policy

- Appendix 1 - List of External Tools;
- Appendix 2 - Purposes of Personal Data Processing;
- Appendix 3 - Information on the Use of Artificial Intelligence;
- Appendix 4 - Cookie Policy.

Appendices 1-4 form an integral part of this Privacy Policy. If there is any inconsistency, the provision that deals more specifically with the relevant issue will prevail, taking into account the applicable agreement and DataMinder's role in the relevant processing activity.

Legal bases and official sources

GDPR - Regulation (EU) 2016/679: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

Polish Electronic Communications Law of 12 July 2024: https://eli.gov.pl/eli/DU/2024/1221/ogl/pol

AI Act - Regulation (EU) 2024/1689: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=en

Standard Contractual Clauses - Commission Implementing Decision (EU) 2021/914: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en

European Commission - adequacy decisions and international transfer frameworks: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

Polish Data Protection Authority - information about rights and complaints: https://uodo.gov.pl/pl/493

APPENDIX 1

LIST OF EXTERNAL TOOLS As at 31 August 2026

Tool	Provider / contracting entity	Purpose and scope	Provider documents
Amazon Web Services (AWS)	Amazon Web Services EMEA SARL	Hosting DataMinder's core infrastructure in the EU (Frankfurt); storing and processing account, project, dataset, file, result and report data; queues, logs and backups; global content delivery and traffic protection through services such as CloudFront and WAF.	Privacy Notice: https://aws.amazon.com/privacy/ AWS Data Processing Addendum and transfer terms: https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html AWS Service Terms, including Standard Contractual Clauses where applicable: https://aws.amazon.com/service-terms/
Microsoft Foundry / Azure OpenAI	Microsoft Ireland Operations Limited	Supporting generative AI features, including processing instructions, conversation history, attachments, dataset descriptions and schemas, statistics, hypotheses, analysis results and errors, and generating interpretations and reports.	Azure legal information: https://azure.microsoft.com/en-us/support/legal/ Microsoft Products and Services Data Protection Addendum, including transfer mechanisms and Standard Contractual Clauses: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA EU Data Boundary and limited operational transfers: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services
Google Workspace (Gmail, Drive, SMTP)	Google Cloud Poland Sp. z o.o.	DataMinder corporate email, SMTP messages to customers, communications and storage of company correspondence and working materials.	Privacy Policy: https://policies.google.com/privacy Google Cloud Data Processing Addendum: https://cloud.google.com/terms/data-processing-addendum EU Standard Contractual Clauses for Google Workspace: https://cloud.google.com/terms/sccs Data Privacy Framework and other transfer mechanisms: https://policies.google.com/privacy/frameworks
Google OAuth	Google Ireland Limited	Optional account registration and login using a Google account.	Privacy Policy: https://policies.google.com/privacy Google API Services User Data Policy: https://developers.google.com/terms/api-services-user-data-policy Data Privacy Framework and Standard Contractual Clauses: https://policies.google.com/privacy/frameworks
Google Analytics 4 (GA4)	Google Ireland Limited	Analytics for DataMinder websites and the application, including traffic, page views, interactions, device information and online identifiers, depending on configuration.	Privacy Policy: https://policies.google.com/privacy Google Analytics Data Processing Terms: https://support.google.com/analytics/answer/3379636 Google Analytics transfer terms and Standard Contractual Clauses: https://support.google.com/analytics/answer/9012600 Data Privacy Framework and other transfer mechanisms: https://policies.google.com/privacy/frameworks
Stripe	Stripe Technology Europe, Limited	Processing one-off payments and supporting paying customers. DataMinder provides the user's email address and name; the user provides Stripe with card details and country or region.	Privacy Center: https://stripe.com/legal/privacy-center Stripe Data Processing Agreement and Data Transfers Addendum: https://stripe.com/legal/dpa Information about the Data Privacy Framework and Standard Contractual Clauses: https://stripe.com/en-be/legal/dpa/faqs
Meta Pixel	Meta Platforms Ireland Limited	Measuring campaign, conversion and advertising performance, subject to configuration and the user's marketing consent.	Privacy Policy: https://www.facebook.com/privacy/policy/ Meta Business Tools Terms: https://www.facebook.com/legal/terms/businesstools Data Processing Terms: https://www.facebook.com/legal/terms/dataprocessing EU-US Data Privacy Framework: https://www.facebook.com/privacy/policies/data_privacy_framework/
Sanity CMS / CDN	Sanity.io	Storing and delivering images used in articles and author profiles. The visitor's browser sends standard request metadata to the CDN, including the IP address and user-agent string.	Privacy Policy and transfer mechanisms, including Standard Contractual Clauses: https://www.sanity.io/legal/privacy Subprocessors: https://www.sanity.io/legal/third-party-subprocessors Terms of Service: https://www.sanity.io/legal/tos
LinkedIn (profile DataMinder)	LinkedIn Ireland Unlimited Company	Operating the DataMinder LinkedIn profile and handling comments and messages sent to it.	Privacy Policy: https://www.linkedin.com/legal/privacy-policy European transfer information, including adequacy decisions, Standard Contractual Clauses and the Data Privacy Framework: https://www.linkedin.com/legal/privacy/eu Standard Contractual Clauses: https://www.linkedin.com/legal/l/eusccs
Facebook and Instagram (DataMinder profiles)	Meta Platforms Ireland Limited	Operating DataMinder Facebook and Instagram profiles and handling posts, comments and messages.	Privacy Policy: https://www.facebook.com/privacy/policy/ Commercial Terms: https://www.facebook.com/legal/commercial_terms EU-US Data Privacy Framework and transfers to Meta Platforms, Inc.: https://www.facebook.com/privacy/policies/data_privacy_framework/
Hotjar	Hotjar Limited	Analysing use of the website or application, including heatmaps, clicks, scrolling and interactions, to improve usability. Hotjar is activated only after consent to analytics cookies.	Privacy Policy and legal documents: https://www.hotjar.com/legal/ Hotjar Data Processing Agreement, including Standard Contractual Clauses for Subprocessors outside the EEA: https://www.hotjar.com/legal/support/dpa/
Fireflies.ai	Fireflies.ai Corp.	Recording, transcribing, summarising and preparing meeting notes after the	Privacy Policy: https://fireflies.ai/privacy-policy

Tool	Provider / contracting entity	Purpose and scope	Provider documents
		required participant consent has been obtained. DataMinder retains meeting materials for three months. Fireflies.ai acts as a Subprocessor where a meeting involves Customer Personal Data.	Data Processing Agreement and transfer mechanisms, including the Data Privacy Framework and fallback Standard Contractual Clauses: https://fireflies.ai/data-processing-agreement Subprocessors: https://trust.fireflies.ai/subprocessors Terms of Service: https://fireflies.ai/terms-of-service

APPENDIX 2

PURPOSES OF PERSONAL DATA PROCESSING As at 31 August 2026

Purpose of processing	Legal basis	Categories of personal data	Retention	Source
Creating and administering an account, authentication and Google login	Article 6(1)(b) GDPR - steps taken at the user's request before entering into the agreement and performance of the Service agreement.	Identification and contact details, account ID, email address, authentication data or OAuth token, login information and account settings.	For the lifetime of the account. After account closure, data is removed from active systems within 30 days, except data required for billing, legal obligations or legal claims. A Google OAuth token is revoked and deleted from active systems when Google login is disconnected or the account is closed; residual backup copies are removed within the ordinary backup cycle and no later than 90 days.	Directly from the user; for Google OAuth, also from Google following the user's choice and authorisation.
Providing DataMinder: projects, data analysis, results and reports	Article 6(1)(b) GDPR - performance of the agreement. Where the user supplies other individuals' personal data, the Controller of that data determines the legal basis.	Account and project data, files and datasets, variable descriptions, instructions, hypotheses, analysis settings, results, charts and reports. The scope depends on the content supplied by the user.	Retained in an active account without a predetermined expiry date. Project or notebook configuration, results and reports are removed from active systems within 30 days, but a separately stored dataset remains until separately deleted. Files, datasets and account data are removed from active systems within 30 days of the relevant instruction; temporary data and caches within 30 days; automated RDS backups within a cycle of no more than 35 days; and logs and LLM traces no later than 90 days.	From the user and from files and data supplied by the user.
Providing AI-based features	Article 6(1)(b) GDPR - performance of the agreement. For Customer Personal Data, processing is carried out on the customer's documented instructions under Article 28 GDPR. Article 50 AI Act imposes transparency requirements but is not an independent legal basis for personal data processing.	Instructions and conversation content, interaction history, attachments, dataset schemas and statistics, hypotheses, analysis results, errors, interpretations and reports. This may include personal data if supplied by the user.	Retained in the active account until the relevant project, notebook, file, dataset or account is deleted. Data is removed from active systems within 30 days of the relevant deletion instruction; application and database logs are retained for one month and LLM traces for no more than 90 days. DataMinder does not use Customer Personal Data to train its own models or for its own research.	From the user, the user's projects and datasets, and outputs generated by the system.
Processing customer datasets containing personal data	Article 28 GDPR - DataMinder acts as Processor on the customer's documented instructions. The customer, as Controller, is responsible for the Article 6 basis and, where relevant, an Article 9(2) condition.	Data contained in customer datasets, files and materials. Direct identifiers and unnecessary data must be removed before upload. Special categories, Article 10 GDPR data and children's data are permitted only after minimisation and at least pseudonymisation, without providing the re-identification key, where the Controller has an appropriate legal basis and safeguards. Effectively anonymised data is outside the GDPR; pseudonymised data remains personal data.	Retained in the active account on the customer's instructions until the relevant project, notebook, file, dataset or account is deleted or the DPA ends. Deleting a project does not delete a dataset stored separately. Data covered by a deletion instruction is removed from active systems within 30 days; automated RDS backups within 35 days; and logs and LLM traces no later than 90 days, unless the law requires continued retention.	From the customer or a person acting on the customer's behalf.
Accounting for Credits and Service use	Article 6(1)(b) GDPR - performance of the agreement.	User and account identifiers, Credit balance and usage history, operation type and time, and related technical identifiers.	For the lifetime of the account and afterwards no longer than until the end of the calendar year in which six years pass after the agreement ends or the relevant claim becomes due, unless a shorter limitation period applies or the period is suspended or interrupted (Articles 118–120 of the Polish Civil Code).	Generated by DataMinder from user activity.
Payments, billing records and tax obligations	Article 6(1)(b) GDPR - performance of the agreement; Article 6(1)(c) GDPR - accounting and tax obligations, including under the Polish Accounting Act and Tax Ordinance.	Identification, contact and billing data; transaction and payment information; country or region; customer and Stripe payment identifiers. Card details are supplied directly to Stripe.	Accounting records: generally five years under Article 74 of the Polish Accounting Act. Tax documents: until the tax liability becomes time-barred, generally five years from the end of the calendar year in which payment was due (Article 70(1) of the Polish Tax Ordinance). Other payment data: for the period necessary to defend claims, generally no longer than the end of the calendar year in which six years pass after the transaction or agreement ends, subject to longer mandatory statutory periods.	From the user, DataMinder systems and Stripe.
Service, account and security communications	Article 6(1)(b) GDPR - performance of the agreement; for security alerts, also Article 6(1)(f) GDPR - legitimate interests in protecting users and the Service.	Name or account name, email address, message content and the account, project, payment or security-event details required for the communication.	For the period required to send and manage the communication and for the lifetime of the account. Where a message evidences contractual performance or a security event, it may be retained for the applicable limitation period, generally no longer than until the end of the calendar year in which six years pass after the agreement ends or the message is sent, subject to suspension or interruption.	From the account, user activity and DataMinder systems.
Customer enquiries, support and error reports	Article 6(1)(b) GDPR where the contact concerns an agreement or pre-contractual steps; Article 6(1)(f) GDPR - legitimate interests in handling correspondence, providing support and improving the Service.	Contact details, correspondence and attachments, and account, project, device, browser, error and user-action information necessary to handle the matter.	Until the matter is closed and then for the applicable claims period, generally no longer than until the end of the calendar year in which six years pass after closure, subject to shorter, suspended or interrupted limitation periods.	Directly from the person contacting us and, in connection with the request, from DataMinder systems.
Complaints, withdrawals, refunds and payment disputes	Article 6(1)(b) and (c) GDPR - performance of the agreement and compliance with legal duties, including the Polish Consumer Rights Act; Article 6(1)(f) GDPR - establishing, exercising or defending legal claims.	Identification, contact, account, order and payment data, request content, correspondence, evidence of Service performance and information required to resolve the matter.	Until the matter is resolved and then until the relevant limitation periods and mandatory accounting or tax retention periods expire.	From the user, DataMinder systems and Stripe, and where relevant from a bank or payment provider.
Security, diagnostics, fraud prevention and demonstrating compliance	Article 6(1)(f) GDPR - legitimate interests in protecting the Service, users and data and in pursuing legal claims; for security obligations, Article 6(1)(c) GDPR in conjunction with	IP address, timestamps, account, session, device and request identifiers, application and security logs, errors	Application, authentication, error, access and security logs, including Lambda and database logs, are retained for one month. LLM traces in self-hosted Langfuse are retained for no more than 90 days.	Automatically from the device, browser, application and DataMinder infrastructure.

Purpose of processing	Legal basis	Categories of personal data	Retention	Source
	Articles 5(2) and 32 GDPR.	and unusual-activity information.	Information isolated as evidence of a specific incident, abuse or proceeding may be retained until the matter ends and then for the applicable claims or proceedings period.	
Waiting list and Service-availability notices	Article 6(1)(a) GDPR - consent. If a message is commercial information or direct marketing, prior consent under Article 398 of the Polish Electronic Communications Law is also required.	Email address, date and wording of consent, and optionally name and information about interest in the Service.	Until consent is withdrawn, the person leaves the list or the waiting-list purpose ends. Evidence of consent and withdrawal may be retained until the end of the calendar year in which six years pass after withdrawal or the purpose ends where needed to demonstrate compliance or defend claims.	Directly from the person joining the list.
Newsletter and email marketing	Article 6(1)(a) GDPR - consent; Article 398 of the Polish Electronic Communications Law - prior consent to commercial information and direct marketing.	Email address, optional name, date and wording of consent, sending history and, where measurement is enabled, opens and clicks.	Until consent is withdrawn or the person unsubscribes. Afterwards, minimum suppression-list data may be retained as necessary to respect the choice, and evidence of consent and withdrawal until the end of the calendar year in which six years pass after withdrawal or the final message where needed to demonstrate compliance or defend claims.	Directly from the subscriber; interaction data from the mailing system.
Recruiting and supporting DataMinder testers	Article 6(1)(a) GDPR - consent; where participation is based on an agreement, Article 6(1)(b) GDPR.	Identification and contact data, tester profile, availability and test progress, feedback, reports, responses and test materials.	Until testing and any participation settlement are complete, and then generally no longer than until the end of the calendar year in which six years pass after completion, settlement or consent withdrawal. Materials unnecessary for settlement or claims are removed earlier.	Directly from the tester and from activity in DataMinder.
Meeting recording, transcription and notes	Article 6(1)(a) GDPR - participant consent. If the content reveals special categories of personal data, an applicable Article 9(2) condition must also be established in a separate assessment.	Voice, image where recorded, identification and contact data, statements, transcripts, notes, summaries and meeting metadata.	Three months from the meeting date. Materials may be deleted earlier following withdrawal of consent where no other basis applies. A specific item may be retained where necessary for legal claims. Following a Fireflies.ai deletion request, permanent deletion is completed under the provider's procedure and no later than 30 days.	From meeting participants and automatically from the meeting-recording tool.
Service analytics and usability research (Google Analytics 4 and Hotjar)	Article 6(1)(a) GDPR - consent; Article 399 of the Polish Electronic Communications Law - prior consent to non-essential storage or access on terminal equipment.	Online and device identifiers, IP address as determined by configuration, approximate location, browser and device data, page views, clicks, scrolling, navigation and other events; for Hotjar, session recordings or heatmaps depending on configuration and masking.	Until consent is withdrawn for future collection. GA4 user and event data is retained for no more than 14 months. Hotjar session recordings and heatmap data are retained for no more than 365 days, after which automatic deletion begins, including from backups. Form data is masked. Withdrawal stops future collection.	Automatically from the device and user activity, only after the required consent.
Campaign and advertising measurement (Meta Pixel)	Article 6(1)(a) GDPR - consent; Article 399 of the Polish Electronic Communications Law - consent to access or store information on the device. Article 398 also applies to direct marketing communications.	Online and advertising identifiers, IP address, browser and device data, visited pages, conversion events and advertising interactions, limited to the active configuration.	Until consent is withdrawn for future collection. No new events are sent after refusal or withdrawal. Meta retains previously received data according to the advertising function, measurement and security requirements and its legal obligations. DataMinder retains available campaign reports while the campaign is run and settled, and afterwards only as long as required for performance analysis or legal claims.	Automatically from the device and user activity, only after the required consent; also from Meta through campaign reports.
Operating DataMinder profiles and handling contact on LinkedIn, Facebook and Instagram	Article 6(1)(f) GDPR - legitimate interests in communication, profile management and relationship building; Article 6(1)(b) GDPR where the contact concerns an agreement or pre-contractual steps.	Profile name, name, public profile information, comments, reactions, messages and other data supplied through the social network.	For the duration of the contact and profile operation. Internal message copies or exports retained as evidence are kept for the applicable claims period, generally no longer than until the end of the calendar year in which six years pass after contact ends. Data remaining on the platform is also subject to the operator's rules.	From the platform user and the relevant social-network operator.
Handling data subject requests	Article 6(1)(c) GDPR - compliance with Articles 12-22 GDPR; Article 6(1)(f) GDPR for documenting the response and defending legal claims.	Identification and contact data, identity-verification information, request content, correspondence, actions taken and data covered by the request.	Until the request is completed. Documentation may be retained until the end of the calendar year in which six years pass after the final response where needed to demonstrate compliance or defend claims, and longer only for ongoing proceedings.	From the requester, their representative and DataMinder systems.
Establishing, exercising and defending legal claims	Article 6(1)(f) GDPR - legitimate interests in protecting DataMinder's rights and defending claims.	Account, agreement, payment, Service-use, communication, report, log and event data necessary for the relevant claim.	Until the applicable limitation period expires and, where proceedings are pending, until they end with final effect and the decision is enforced.	From the person concerned, DataMinder systems, payment or Service providers and, where relevant, authorities, courts and legal representatives.
Recording and demonstrating consent and privacy preferences	Article 6(1)(c) GDPR in conjunction with Articles 5(2) and 7(1) GDPR - demonstrating compliance; for technology and communication consent, also Articles 398-399 of the Polish Electronic Communications Law.	User or device identifier, consent type and wording, date and time, notice version, preferences and information about withdrawal or amendment.	For as long as the preference applies. Evidence of consent, refusal, amendment or withdrawal may be retained until the end of the calendar year in which six years pass after the last amendment or withdrawal where needed to demonstrate compliance or defend claims. A minimum suppression-list entry may be retained as long as necessary to respect an objection.	Directly from the user's choice and automatically from the consent-management mechanism.

APPENDIX 3

Information on the Use of Artificial Intelligence

As at 31 August 2026

1. AI features in DataMinder

DataMinder uses artificial intelligence systems as a supporting layer in its data-analysis Service. The relevant interface informs Users when they are using an AI feature. AI supports, in particular:

- conversations and clarification of the research question;
- formulation and refinement of hypotheses;
- creation of textual explanations, interpretations and reports based on calculated results;
- generation of titles, descriptions, supporting content and project elements;
- explanation of errors and presentation of analysis results.

Statistical calculations are performed by a separate deterministic component. The language model is not the source of statistical values or statistical test results; it receives calculated results so that it can present and explain them in natural language.

2. Provider and component used

DataMinder uses Microsoft Foundry / Azure OpenAI for generative AI features. The contractual entity identified in DataMinder's documentation is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland. A model from the GPT family is used.

Data is provided to the supplier only to the extent necessary to perform the feature initiated by the User. Current information about the supplier and its documents is available in Appendix 1 to the Privacy Policy - List of External Tools.

> The Azure OpenAI deployment assigned to DataMinder operates in the EU Data Zone Standard. Model inputs and outputs are processed within that data zone in accordance with the Service configuration. Microsoft provides for limited global access or transfers connected, among other things, with security, support and Service maintenance. In those circumstances, the mechanisms and safeguards set out in the Microsoft DPA and Chapter V GDPR apply.

3. Information that may be processed by AI features

- messages, questions and instructions from the User, and conversation history;
- attachments and information extracted from uploaded files;
- dataset descriptions, field names and types, schemas, statistics and value samples;
- hypotheses, project context, analysis results and error information;
- generated responses, reports, text, code and technical execution metadata.

The scope depends on the content provided by the User. Materials may include personal data, confidential information or data from a customer dataset. Users should provide only information necessary for the relevant purpose and, where they act as a Controller, must have an appropriate legal basis for processing.

Before providing data, Users must remove direct identifiers and information that is unnecessary for the analysis. Special categories of personal data, data relating to criminal convictions and offences, and children's data may be processed only after minimisation and at least pseudonymisation, without providing DataMinder with the re-identification key, where the User has an appropriate legal basis and safeguards proportionate to the risk. Properly anonymised data is not personal data; pseudonymised data remains subject to the GDPR.

4. Roles and responsibility for data

For account, billing and security data and its own operational purposes, DataMinder acts as a Controller. For personal data included in a customer dataset, DataMinder generally acts as a Processor on the customer's documented instructions, in accordance with Article 28 GDPR and the applicable DPA.

As Controller, the customer is responsible in particular for the lawful collection of data, the applicable legal basis, compliance with transparency obligations, determination of an appropriate retention period and the lawfulness of the intended use of the results.

DataMinder is responsible for obligations relating to the deployment and use of AI features to the extent arising from the role attributed to it under the AI Act. The assessment depends on the specific feature, manner of integration, intended purpose and changes made to the system, and is updated when those elements change.

5. Transparency and identification of AI use

Features intended to interact directly with a User should clearly indicate that the response or content is generated by AI, unless this is obvious to a reasonably well-informed, observant and circumspect person in the circumstances. The information should be provided no later than when the interaction begins.

This obligation arises under Article 50(1) AI Act, which applies from 2 August 2026. The scope of obligations concerning machine-readable marking of AI-generated or AI-manipulated content requires a separate assessment under Article 50(2) AI Act and current European Commission guidance.

The interface of features intended for direct interaction informs the User that they are interacting with AI. AI-generated or AI-manipulated content is marked to the extent required by Article 50 AI Act, taking account of the type of content and how it is made available.

6. Human oversight and use of outputs

- AI outputs are intended to provide support and may require verification by the User;
- the User should check the accuracy of input data, assumptions, interpretations and the generated report;
- AI output should not be treated as professional legal, medical, financial or other specialist advice;
- if there is any discrepancy, the results of deterministic statistical calculations prevail over the language model's textual explanation.

Under the current design, DataMinder does not use AI to make decisions concerning a User that are based solely on automated processing and produce legal effects or similarly significantly affect that User. If the way in which the product is used changes, Article 22 GDPR and the AI Act classification will need to be reassessed.

7. Restrictions and prohibited uses

AI-generated content may be incomplete, inaccurate, out of date or inappropriate to the context. Human oversight alone does not eliminate the risk of error or establish that a particular use is lawful.

Without a prior documented legal, risk and safeguards assessment, DataMinder should not be used to make or support decisions concerning specific individuals in areas such as:

- recruitment, employment, employee evaluation or termination of employment;
- admission to education or assessment of pupils or students;
- access to credit, insurance, public benefits or essential services;
- diagnosis, treatment or other medical decisions;
- risk profiling, individual scoring, law enforcement or the administration of justice;
- emotion recognition, biometric categorisation or other uses that may be prohibited or subject to the AI Act high-risk regime.

8. Training, product improvement and retention

According to Microsoft's public information, Azure OpenAI customer data is not used to train the provider's foundation models without the customer's permission. This public statement does not replace verification of the terms and settings applicable to DataMinder's specific account.

DataMinder processes prompts, responses and metadata to the extent necessary to provide AI features, account for usage, perform diagnostics, maintain security and generate reports. Customer Personal Data is not used by DataMinder to train its own models or for benchmarking, research, marketing or product improvement unless this has been separately and lawfully agreed. The applicable legal bases, purposes and retention periods are described in the Privacy Policy and Appendix 2 - Purposes of Personal Data Processing.

> Prompts, responses and project data remain in the active account until deleted on the User's instructions. Application and database logs are retained for one month, LLM traces for no more than 90 days and automated RDS backups on a cycle of no more than 35 days. Detailed retention criteria are provided in Appendix 2.

9. Data security and minimisation

Before uploading data, the User should limit it to what is necessary for the analysis and, where possible, remove direct identifiers, apply pseudonymisation and avoid including personal data in project names, field names or instructions. Pseudonymisation is not anonymisation and does not disapply the GDPR.

DataMinder applies the technical and organisational measures described in the Service documentation. Detailed security parameters should not be inferred from this information; binding commitments arise from the applicable agreement and security documentation.

10. Individual rights and contact

Information about the Controller, legal bases, recipients, transfers, retention and individual rights is provided in the Privacy Policy and its other appendices. Where DataMinder processes data on a customer's behalf, requests relating to the customer's dataset are handled in accordance with the roles set out in the applicable DPA.

Questions about the use of AI or personal data may be sent to contact@dataminder.ai.

Regulatory basis and official materials

AI Act - Regulation (EU) 2024/1689, in particular Articles 4, 5, 50 and 113: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=en

European Commission - Guidelines on Article 50 AI Act transparency obligations, 20 July 2026: https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems

Microsoft EU Data Boundary - limited transfers for all services: https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services

Microsoft Products and Services Data Protection Addendum: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

GDPR - Regulation (EU) 2016/679, in particular Articles 5, 6, 9, 13-14, 22, 25, 28 and 32: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

APPENDIX 4

COOKIE POLICY Version DM-COOKIE-310826-EN | As at 31 August 2026

1. Scope of this document

This Cookie Policy explains how DataMinder sp. z o.o. uses cookies, local storage, session storage and similar technologies on DataMinder websites and in the DataMinder application. It supplements the Privacy Policy and the List of External Tools.

The Controller of personal data associated with these technologies for DataMinder's own purposes is DataMinder sp. z o.o., with its registered office at ul. Lipnowska 207, 09-400 Maszewo Duże, Poland. Contact: contact@dataminder.ai.

2. What are cookies and similar technologies?

Cookies are small pieces of information stored by a web browser. Local storage and session storage operate in a similar way. These technologies may be used to maintain a login session, remember settings, secure payments, measure use of the Service and assess campaign performance.

The period indicated below is the maximum time for which information remains on the device. The User may remove it earlier. The provider may retain data for a different period, as described in its documentation and, for personal data, in the Privacy Policy.

3. Giving and withdrawing consent

Necessary technologies are used without separate consent only to the extent required for transmission, to provide a feature expressly requested by the User, for authentication or security, or to remember the User's privacy choice.

Google Analytics 4, Hotjar and Meta Pixel remain disabled until the relevant consent is given. They do not transmit data before consent, after consent is refused or after consent is withdrawn. Analytics and marketing consents are separate.

Consent may be changed or withdrawn at any time by reopening the cookie-settings panel available through the Service. Withdrawal does not affect the lawfulness of earlier processing. Refusing consent does not restrict access to DataMinder's core features.

Optional technologies rely on consent under Article 399 of the Polish Electronic Communications Law and, where personal data is processed, Article 6(1)(a) GDPR. Necessary technologies rely on the exemption in Article 399(3) of that Law; the corresponding legal basis for processing personal data is, as applicable, performance of the agreement or DataMinder's legitimate interest in maintaining the security and proper operation of the Service.

4. Technologies used by DataMinder

4.1. Necessary technologies and User-selected settings

Technology	Purpose and scope	Duration
DataMinder authentication cookie	Maintains the logged-in session, authenticates the user and protects the account.	Up to 30 days
Interface settings	Remembers interface settings selected by the user.	Up to 7 days

Technology	Purpose and scope	Duration
Language preference	Remembers the selected Service language.	Up to 1 year
Cookie choice - local storage	Records consent, refusal or withdrawal so that the user's choice can be respected.	Until the choice is changed or browser storage is cleared
Bookmark state - local storage	Maintains the state of user-selected interface elements.	Until the setting is changed or browser storage is cleared
Stripe: __stripe_mid	Fraud prevention and risk assessment when the user initiates a payment.	Up to 1 year
Stripe: __stripe_sid	Fraud prevention and protection of the current payment session.	Up to 30 minutes
Stripe: __stripe_ab, __stripe_mf - session storage	Payment protection and fraud detection on Stripe pages.	Until the end of the session

Stripe cookies are activated when the User initiates a payment. Depending on the payment method, device and fraud-prevention mechanisms, Stripe may also use other technologies necessary to secure the payment process.

4.2. Analytics and usability research

The following technologies are activated only after analytics consent has been given.

Technology	Purpose and scope	Duration
GA4: _ga	Distinguishes users and measures use of the Service.	Up to 2 years by default; the browser may shorten this period
GA4: _ga_<container-id>	Maintains session information and attributes events to the relevant session.	Up to 2 years by default; the browser may shorten this period
Hotjar: _hjSessionUser_<site-id>	Assigns repeat visits to a pseudonymous identifier specific to the DataMinder Service.	Up to 365 days
Hotjar: _hjSession_<site-id>	Maintains current-session data used for heatmaps and interaction analysis.	30 minutes, extended by activity
Hotjar test cookies and storage	Tests cookie, local-storage and session-storage support and view parameters, including _hjCookieTest, _hjLocalStorageTest, _hjSessionStorageTest and _hjTLDTest.	For the session or deleted almost immediately after the test

4.3. Campaign measurement and marketing

The following technologies are activated only after marketing consent has been given.

Technology	Purpose and scope	Duration
Meta Pixel: _fbp	Identifies the browser for advertising measurement, conversion measurement, marketing analytics and, depending on the configuration, remarketing.	Up to 90 days

Technology	Purpose and scope	Duration
Meta Pixel: _fbc	Stores the Meta advertising click identifier where the user reaches DataMinder through an advertisement containing that identifier.	Up to 90 days

5. Data that may be processed

Depending on the technology, the following information may be processed: a cookie or device identifier, IP address, date and time of the visit, pages visited, clicks, scrolling activity, session parameters, browser, operating-system and device information, approximate location, referral source and information about campaign performance. DataMinder does not send dataset content or direct User identifiers to analytics or marketing tools.

6. Providers and transfers

The providers of technologies described in this Policy include Google Ireland Limited, Hotjar Limited, Meta Platforms Ireland Limited and Stripe Technology Europe, Limited. Further information about the entities, purposes, provider documents and potential transfers outside the EEA is provided in Appendix 1 to the Privacy Policy.

7. Managing technologies in the browser

In addition to using the cookie-settings panel, Users can delete or block cookies through their browser settings. Blocking necessary technologies may prevent login, settings, payments or other features from working properly. Deleting cookies in the browser does not necessarily delete data previously sent to a provider.

8. Changes to this Policy and contact

This Policy may be updated following changes to the law, Service configuration, technologies used or providers. The current version is published through the DataMinder Service. Questions about cookies and data protection may be sent to contact@dataminder.ai.

9. Provider documentation

- Google Analytics - GA4 cookies: https://support.google.com/analytics/answer/11397207
- Hotjar - tracking-code cookies: https://help.hotjar.com/hc/en-us/articles/36819973371409-Cookies-Set-by-the-Hotjar-Tracking-Code
- Meta - Cookie Policy: https://www.facebook.com/privacy/policies/cookies/
- Stripe - cookie settings and list: https://stripe.com/cookie-settings