PRIVACY POLICY OF THE DEEP DIGITAL EVIDENCE ECOSYSTEM & PROTOCOLS PLATFORM

Version: April 30th, 2026

1. PURPOSE

At DEEP Measures Oy (Business ID 3310723-4), a Finnish limited liability company with its registered office at Lapinlahdenkatu 16, 00180 Helsinki, Finland ("**DEEP**", "**we**", "**our**", "**us**"), we are committed to protecting your privacy and handling personal data in accordance with applicable data protection laws, including the EU General Data Protection Regulation ("**GDPR**").

Our Digital Evidence Ecosystem & Protocols platform ("**Platform**") provides a catalogue of digital measures and measurement solutions and a collaborative framework intended to support the development and evaluation of digital measurement solutions that improve regulatory and evidence-based decision-making.

This Privacy Policy explains how we collect, use, disclose and protect personal data when you use our Platform or Services, and when you interact with us in connection with our marketing, sales activities, customer agreements, recruitment processes, or when visiting our website.

DEEP acts under two distinct roles in accordance with the General Data Protection Regulation (GDPR):

- As a **Data Processor**, when we process personal data on behalf of our members or clients (the "Data Controllers") through the Platform.
- As a **Data Controller,** we process personal data for our own purposes, such as website management, marketing, human resources, or supplier and customer relations.

This Privacy Policy explains how DEEP processes personal data in both roles, the security measures we apply, and how individuals can exercise their rights.

2. DESCRIPTION OF DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA

Processing of personal data concerns the following categories of data subjects:

- Users of our Platform (i.e. our Customers' employees);
- Website visitors; and
- Representatives of our customers.

Only personal data that is necessary for the purposes described in this Privacy Policy is processed, in accordance with the principle of data minimization.

We collect the following personal data through different means when you use our Platform or interact with Us. The type of data collected depends on the data subject and varies by assignments. This includes, but is not limited to the following:

- basic information, such as name, date and place of birth and contact details (email address, phone number);
- information relating to our relationship, such as services and order details, contract information, payment details, billing information;
- service-related information, e.g. user IDs, authentication credentials as well as data generated in connection with service provision e.g., login information, and how services are used;
- project related data such as data of the participants to the missions;
- your communication and interactions with us, such as correspondence, and service requests;
- conversational and query data, including prompts, questions, and interactions submitted by users through the Platform's AI Features (chat interface and embedded action buttons), and any Agent Outputs generated in response; and
- other data, which is based on your consent and defined in detail on a case-by-case basis.

As part of our recruitment process, we also collect and process data, which:

- Is generated or provided by you during the recruitment process (e.g. when you fill out an application form or provide information about you in an interview, or provide your CV);
- Is obtained from publicly available sources or third parties, to the extent permitted by applicable laws e.g. from your referees, recruitment consultants and external websites (e.g. LinkedIn) or for which you have provided consented.

We may combine the data collected from various sources, e.g. from publicly available sources, and from your CV. You may decide not to provide any personal data to us, but we may not be able to proceed with the recruitment process with you.

We may collect and use for any purpose aggregated data and metadata of the Platform, where individual person is not identified, e.g., statistical data collected in connection with the use of our Platform. Such aggregated or anonymized data no longer constitutes personal data.

Retention criteria: We retain personal data for the duration of the contractual relationship and thereafter for as long as necessary to comply with applicable legal, regulatory, accounting or contractual obligations. After that, we will securely dispose of your personal data by deletion or anonymization in accordance with applicable laws and internal policies. With your consent, we may process your personal data for future open positions for a specified period of two (2) years. With your consent, this period may be extended for future open positions. Such consent may be withdrawn at any time.

We do not collect any health or patient data (data collected from patients in a clinical trial). Members are prohibited from submitting personal data, special category data (as defined under Article 9(1) GDPR), patient data, or data subject to any regulatory frameworks, including but not limited to data regulated under HIPAA (US health data), the Data Protection Act 2018 (UK), CCPA (California Consumer Privacy Act) or any equivalent national or sectoral legislation governing the processing of personal or sensitive data through the Platform's AI Features. Any such data submitted in breach of this prohibition remains the sole responsibility of the Member.

We do not knowingly collect personal data from children under the age of 16. If we become aware that we have collected personal data from a child without appropriate consent, we will take steps to delete such information and, where necessary, seek parental consent.

3. MARKETING AND ANALYTICS

We may market and inform you about our Platform and services. We may combine the data collected from our different interactions with you. Furthermore, your personal data may also be used for market research and customer surveys.

Processing of personal data for general business-to-business (B2B) marketing and customer relationship management purposes is based on our legitimate interest (Article 6(1)(f) GDPR), in order to collect and analyse relevant information to better understand our customers and to develop our Platform and related services. You have the right to object to such processing at any time by contacting us or by using the unsubscribe option included in our communications.

We may track interactions with our marketing emails, such as email opens and link clicks, to measure and improve the effectiveness of our communications. This engagement tracking is applied primarily to marketing and informational emails, including newsletters, service updates, or event invitations. One-to-one or individual email communications may not include tracking and are generally used solely for direct correspondence.

The processing of this data is based on our legitimate interest in managing and improving our communications, or, where applicable, on your consent. You can opt out of this tracking at any time, and if you no longer wish to receive marketing emails from us, you may unsubscribe by clicking the “unsubscribe” link included at the bottom of our emails or by contacting us directly. Your preferences will be respected, and you will be removed from future marketing communications. You have the right to object at any time to the processing of your personal data for direct marketing purposes. Where processing is based on your consent, you may withdraw that consent at any time. You may exercise these rights by using the unsubscribe link included in our communications or by contacting us in accordance with Section 13 (Contact Us) of this Privacy Policy.

4. PURPOSE AND LEGAL BASIS FOR PROCESSING OF PERSONAL DATA

We collect and process your personal data for the purposes of providing our Platform to you and fulfilling our contractual obligations to you, as well as for other legitimate business purposes, such as improving our services and communicating with you about our products and services.

The legal basis for processing your personal data may vary depending on the specific purposes for which we are processing your data, but may include your consent, our legitimate interests for performance of the contract, or compliance with legal obligations.

We use your data for the following purposes, among others:

- Keeping our Platform running - providing services to you and ensuring the functioning and maintenance of Platform;
- Verifying your identity for the purposes of signing into the Platform;
- Improving our Platform, products, services, marketing, and your experience;

- Interacting with You for feedback on our services;
- Managing recruitment process, evaluating suitability of job applicants, improving our recruitment process and for statistical and recordkeeping purposes;
- Improving and personalizing services and to develop new services and providing notifications on new features, changes, and improvements, including informative communications related to the functionalities, products, or contracted services, including the security updates, when necessary or reasonable for their implementation
- Managing, pursuing, analysing, and improving the customer relationship with you, including customer communication, user account management and processing payments;
- Customer Support, corresponding with users, solving issues, and providing customer support;
- Informing and interacting with you of new services, features, and content we may offer;
- Providing AI-powered assistance through the Platform's AI Features, including the chat interface and embedded action buttons, by processing user queries, prompts, and Platform content, and publicly available web sources to generate Agent Outputs. The legal basis for this processing is performance of contract (Article 6(1)(b) GDPR) and legitimate interests (Article 6(1)(f) GDPR), to the extent that publicly available web sources contain personal data, such as author attribution in published works; as AI Features form part of the Platform services; and
- For other purposes, such as data analysis, identifying usage trends and determining the effectiveness of our promotional campaigns.

We may process your personal data also for specific purposes if you have provided consent to such processing.

5. DATA SHARING AND DISCLOSURES OF PERSONAL DATA

We may share your personal data with third-party service providers who assist us in providing our services. We may also disclose your personal data to comply with legal obligations or to protect our legal interests.

All sub-processors are contractually bound under Article 28 of the GDPR to maintain confidentiality, security, and process data only for the specified purposes.

6. USE OF COOKIES

When you visit our website and platform, cookies, and other similar technologies ("**Cookies**") are used to automatically collect information about your visit. Cookies help us operate, improve, and personalize your experience, but we only use optional cookies with your explicit consent.

Website Cookies

It is possible for you to accept or refuse the use of cookies through our cookie banner. We use the following types of cookies on our website to enhance your browsing experience and to better understand our website's performance. Some cookies on our website are set and managed automatically by our service providers, including HubSpot (for website analytics, marketing forms, and contact management) and Cloudflare, which provide website functionality, analytics, consent management, and security services. These cookies cannot be individually configured by us.

Necessary Cookies: These cookies are essential for the operation of our website. They enable core functionalities such as security, network management, and accessibility. You cannot disable these cookies, but you can set your browser to block or alert you about these cookies.

Necessary cookies used to record your consent choices are required to ensure that we respect your preferences and comply with applicable data protection and privacy laws Typical retention periods for necessary cookies are:

- Consent and preference cookies: up to 6 months
- Security and infrastructure cookies (e.g. Cloudflare): 30 minutes or session-based

Statistics Cookies: These cookies allow us to measure and improve the performance of our website. They help us understand how visitors interact with our website by collecting and reporting information anonymously.

Statistics cookies are only set where you have provided consent via the cookie banner. Typical retention periods for statistics (analytics) cookies are:

- Visitor identifiers and analytics cookies: up to 6 months
- Session cookies: approximately 30 minutes or for the duration of the session

We rely on your consent for the use of optional cookies (e.g. analytics), in accordance with Article 6(1)(a) GDPR and Article 5(3) of the ePrivacy Directive. Consent is obtained through our cookie banner upon your first visit to our website.

You can withdraw or modify your consent at any time by accessing the cookie settings available on our website.

Accepting optional cookies will enable you to get the best from our website. Refusing optional cookies will not affect the use of necessary cookies required for core site functionality, but some features, such as analytics, may be unavailable.

Platform Cookies

We use the following types of cookies in our platform:

Necessary Cookies: These cookies are used primarily for authentication and user session management. They store necessary data to ensure secure and seamless access to our Platform. You cannot refuse these cookies. The retention time for necessary cookies is one (1) month.

The key information stored in our authentication cookies includes, for example:

- Authentication Tokens: Access tokens for the DEEP Platform;
- Session Management: Refresh token to maintain user login status;

- User Profile Information: First name, last name, and organization ID; and
- Customization & Preferences: User default workspace and accepted Terms of Use and Privacy Policy version.

Analytics Cookies: We may use Microsoft Clarity for analytics purposes to improve the platform and its content for you. Clarity cookies collect data such as clicks, scrolling, mouse movements, session identifiers, approximate geolocation data (city and country), and other behavioural metadata to improve usability, functionality, and performance. No confidential customer data is collected for analytics. Data collected via Clarity cookies is retained according to Microsoft's retention policies: session recordings for approximately 30 calendar days, and aggregated interaction data (heatmaps, clicks) for up to approximately 13 months. Data is automatically deleted after the applicable retention period. Analytics cookies are also retained for 13 months. All data and cookies are automatically deleted after their respective retention periods. You can withdraw or modify your consent at any time via the user profile in the platform or by contacting info@deepmeasures.health. Declining analytics means no analytics data will be collected, and the DEEP Platform will still work as normal.

7. TRANSFER OF PERSONAL DATA OUTSIDE OF THE EU OR EEA

The data we collect is processed by Us within the European Union (EU)/European Economic Area (EEA) and in third party data processing facilities within the EU/EEA.

Some of our service providers may have access or are located outside the EU/ EEA and their processing of your personal data will involve a transfer of data outside of EU/EEA.

We ensure that such international transfers are made only under appropriate safeguards, including:

- Transfer to countries that have been deemed by the European Commission to provide an adequate level of data protection, or
- Use the Standard Contractual Clauses (SCCs) adopted by the European Commission under the Article 46(2)c of the GDPR, together with additional technical, organisational and contractual measures where necessary, to ensure that your personal data enjoys the same level of protection as within the EU/EEA.

8. USE OF SUB-PROCESSORS

8.1 We may engage third-party service providers, known as sub-processors, to process personal data on our behalf in connection with the operation and provision of the Platform and related services. These sub-processors help us deliver, maintain, and improve our services, and include cloud providers, analytics tools, and project management services.

8.2 All sub-processors are carefully selected and are bound by contractual obligations to process personal data only for the specific purposes required to provide our services and to maintain the same level of data protection as described in this Privacy Policy.

8.3 Currently, our primary sub-processors include:

8.3.1 Microsoft 365: Provides document management, intranet, collaboration, and communication services for the Platform. Personal data processed includes user

credentials, profile information, documents, and communications related to Platform usage. Data is processed in EU-selected data centers.

8.3.2 Microsoft Azure: Provides cloud computing, infrastructure, storage, and hosting services for the Platform. Personal data processed includes Platform content, authentication data, logs, and system data. Data is processed in EU-selected data centres. Microsoft Azure also provides the infrastructure for the Platform's AI Features, including the processing of user queries, prompts, and Platform content through Azure-hosted large language models and Retrieval-Augmented Generation (RAG) technology. Data processed in connection with AI Features is encrypted in transit and at rest, is segregated from other customers' data, and is not used to train Microsoft's underlying models. AI processing is performed within EU-selected data centers.

8.3.3 Microsoft Azure AI Foundry: Provides the large language model capabilities, orchestration, and deployment infrastructure that power the Platform's AI Features, including the chat interface, purpose-built agents, prompt pipelines, and retrieval-augmented generation workflows. Personal data processed includes user queries, prompts, and conversational inputs submitted through AI Features. Data is processed within EU-selected Azure data centers, is encrypted in transit and at rest, and is segregated from other customers' data. Customer data is not used to train underlying models. Microsoft's data processing terms apply and are available upon request.

8.3.4. Microsoft Clarity: Provides behavioural analytics for the Platform interfaces. It collects and processes user interaction data, including clicks, scrolling, mouse movements, session identifiers, and other behavioural metadata, to understand how the Platform is used and to improve usability, functionality, and user experience. No data is collected before end users provide explicit consent. Consent for processing via Microsoft Clarity is obtained on behalf of your organization (the Data Controller). The Platform facilitates the collection and recording of consent. No confidential customer data is collected for analytics. End users may withdraw their consent or object to processing at any time via the privacy settings, or by contacting info@deepmeasures.health. Refusing or withdrawing consent will not prevent users from using the Platform. It will continue to function as normal.

8.3.5 Mango Technologies Inc. (dba ClickUp): Provides project management and help desk tools for internal and customer-facing activities. Personal data processed includes task assignments, project details, communication records, and related metadata. Data is processed in EU-selected data centers.

8.3.6 HubSpot, Inc.: Provides customer relationship management (CRM), email communication, website analytics, and contact management services. Personal data processed may include names, email addresses, organization details, communication history, and interaction data (such as email opens, link clicks, and website visits). HubSpot processes this data on behalf of DEEP to support communications with users, including notifications about platform updates, new features, and service announcements, ensuring optimal service delivery. Personal data is processed and stored in selected data centers within the European Union. HubSpot ensures GDPR-compliant safeguards for data transfers and processing, including the Standard Contractual Clauses (SCCs) adopted by the European Commission.

8.4 We maintain an up-to-date list of all sub-processors on our website. Customers may also request access to this list or obtain further information about the processing performed by

contacting us at info@deepmeasures.health any time. We will notify customers in advance of any intended changes to the list, thereby providing the opportunity to object to such changes in accordance with Article 28 (2) GDPR.

9. RETENTION OF PERSONAL DATA

We will retain your personal data only for as long as necessary to provide services to you and for as long as necessary to comply with applicable legal, regulatory, accounting, or contractual obligations. After that, we will securely dispose of your personal data by deletion or anonymization in accordance with applicable laws and internal policies.

With your consent, we may process your personal data for future open positions for a specified period of two (2) years. With your consent, this period may be extended for future open positions. Such consent may be withdrawn at any time without affecting the lawfulness of processing based on consent before its withdrawal.

Data collected via Microsoft Clarity is retained in accordance with Microsoft's retention policies, which include session recordings retained for approximately 30 calendar days and click/heatmap or labelled session data retained for up to approximately 13 months. All data and cookies is automatically deleted after the applicable retention period expires in accordance with Microsoft's policies, and processing remains compliant with the GDPR and other applicable data protection laws.

Conversational and query data submitted through AI Features, including chat messages, prompts, and conversational Agent Outputs, is deleted at the end of the active session unless the Member has reported an issue and has provided explicit consent to the retention of that session data for the purposes of investigation and quality assurance. Where such consent is given, data is retained for a period of up to ninety (30) days from the date of consent, after which it is securely deleted or anonymized. Members may withdraw consent and request earlier deletion at any time by contacting us at info@deepmeasures.health.

We may also retain and process your personal data to comply with our statutory obligations and to establish, exercise, or defend legal claims, including, where applicable, in connection with employment, contractual, or discrimination-related matters.

If you have provided your consent to the collection and processing of your personal data in connection with the recruitment process, you have the right to withdraw your consent for that specific processing at any time. If you wish to withdraw your consent, you may contact info@deepmeasures.health.

10. YOUR RIGHTS

You have certain rights regarding your personal data:

Right to Access: You have the right to access your personal data that we hold.

Right to Rectify Personal Data: You have the right to request that we correct any inaccurate or incomplete personal data that we hold.

The Right to Object to the Processing: You have the right to object to the processing of your personal data for certain purposes.

The Right to Data Portability: You have the right to receive your personal data in a structured, commonly used, and machine-readable format.

The Right to Be Forgotten: You have the right to request that we erase your personal data under certain circumstances.

The Right to Restriction of the Processing: You have the right to request that we restrict the processing of your personal data under certain circumstances.

The Right to Give and Withdraw Your Consent: You have the right to give or withdraw your consent for the processing of your personal data.

11. DATA SECURITY

We take appropriate technical and organizational measures to protect your personal data from unauthorized access, disclosure, or other misuse. These measures include physical, electronic, and procedural safeguards that comply with applicable legal requirements.

Our Platform is running in Microsoft Azure cloud. Microsoft Azure provides various security measures and controls to help protect members' data, including network security, identity and access management, encryption, and monitoring.

To ensure information security and data protection for the Platform, access control mechanisms are implemented to restrict access to data to authorized personnel only. Data is encrypted both in transit and at rest, and secure protocols are used.

Although our good faith efforts to store your data in a secure operating environment that is not available to the public, please remember that unfortunately no data transmission or storage is 100% risk free. You provide your personal data at your own risk, and we cannot guarantee the absolute security of your data. In the unfortunate case of a security breach that endangers your privacy or data we will inform you as well as the relevant authorities, as required by law. We may also temporarily shut down services to protect the personal data.

12. CHANGES TO THE PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our data processing practices, applicable laws, or services. The updated version will be published on our website and will apply from the date of publication. We encourage you to review this Privacy Policy periodically to stay informed about how we protect your personal data.

13. CONTACT US

If you have any questions or concerns about this privacy policy or our use of your personal data, please contact us at:

- Address: Lapinlahdenkatu 16, 00180 Helsinki, Finland
- Email: info@deepmeasures.health

You also have the right to lodge a complaint with the competent supervisory authority in Finland, which is the Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto). Further information is available at https://tietosuoja.fi/en/home.

You may also lodge a complaint with your local supervisory authority.