DeepHealth, Inc. – GDPR Website Processing Annex

This Annex supplements the DeepHealth, Inc. Website Privacy and Cookies Notice (ISN-001) and summarizes the categories of personal data processed via our websites, the purposes, legal bases under the GDPR and UK GDPR, sources, recipients, retention periods, international transfer safeguards, and key restrictions. It applies only to website-related processing described in ISN-001 and does not cover clinical products or protected health information.

Category of Personal Data	Purposes of Processing	Legal Basis (Art. 6 GDPR / UK GDPR)	Special Categories / Art. 9 Basis	Sources	Recipients / Categories of Recipients	Retention	International Transfers & Safeguards	Notes & Restrictions
Identifiers and contact data (e.g., name, email address, phone number, organization, role)	• Respond to inquiries and requests submitted via web forms. • Manage relationships with prospects, customers, suppliers, and partners. • Register and administer online events and webinars. • Provide service-related communications and respond to support requests. • Send marketing communications where permitted and where consent is obtained when required by law.	• Art. 6(1)(f) – Legitimate interests in operating and securing websites, responding to inquiries, and managing business relationships (balanced against data subject interests). • Art. 6(1)(a) – Consent for electronic marketing communications where required by law. • Art. 6(1)(c) – Compliance with legal obligations (e.g., record keeping, regulatory correspondence).	Not applicable (identifiers and basic contact data are not treated as special categories in this context).	• Directly from individuals when they submit forms or contact us via the website. • From event registration pages and landing pages integrated with our website. • From business-to-business contact enrichment providers as permitted by law.	• Website hosting, CRM, marketing automation, event management, and customer support service providers acting as processors. • Corporate affiliates assisting with website operations. • Event co-hosts and promotional partners when clearly disclosed at registration. • Professional advisors (e.g., legal counsel, auditors) where necessary.	• Contact form submissions: retained for the life of the case plus 24 months. • Marketing preference records: retained until you unsubscribe, 24 months after your last engagement, or as long as needed to honor opt-out choices. • Rights request records: retained in accordance with legal and audit obligations.	• Personal data may be transferred outside the EEA/UK, including to the United States. • Where required, transfers rely on mechanisms such as the EU Standard Contractual Clauses and the UK International Data Transfer Addendum, supported by transfer impact assessments.	• Website is not intended for submission of medical or patient information; individuals are instructed not to submit PHI through website forms. • Data is not sold for monetary consideration. Any "sale" or "sharing" concepts under U.S. law are handled via separate state-law disclosures and opt-out mechanisms.
Online identifiers and technical logs (e.g., IP	• Provide, operate, and secure websites and online	• Art. 6(1)(f) – Legitimate interests in operating	Not applicable (data in this category is not	• Automatically from browsers	• Hosting providers, content delivery networks,	• Web server and security logs: retained	• Technical logs and security data may be stored or accessed	• Only strictly necessary cookies and tags are set

address, device identifiers, user agent, timestamps, URL requests); strictly necessary cookies and similar technologies	services. • Enable core site functionality (e.g., page navigation, session management, load balancing). • Detect, prevent, and investigate security incidents, abuse, and fraud. • Maintain log records necessary for security monitoring and forensic analysis.	secure websites, preventing abuse, and ensuring availability and integrity of services. • Art. 6(1)(c) – Compliance with legal obligations related to security, logging, and incident response where applicable.	processed as special categories).	and devices when individuals access the website. • From security and performance tools integrated with our hosting infrastructure.	and security service providers (e.g., firewalls, DDoS protection, WAF, monitoring tools) acting as processors. • Corporate affiliates providing infrastructure support. • Public authorities or law enforcement when required by law.	for approximately 12 months. • Aggregated location analytics derived from IP address: retained for up to 14 months. • De-identified technical data may be retained longer where it can no longer reasonably identify individuals.	outside the EEA/UK, including in the United States. • Transfers are subject to appropriate safeguards (e.g., Standard Contractual Clauses and UK Addendum) and security controls defined in the ISMS.	before consent. • We do not use this category of data for marketing, profiling, or targeted advertising. • No geofencing is used to identify or target individuals seeking in-person healthcare services.
Analytics and marketing identifiers (e.g., analytics cookies, advertising cookies, SDK and pixel IDs, consent preferences)	• Measure and analyze website performance, usage patterns, and user experience. • Improve site content and navigation. • Deliver personalized or interest-based advertising where consent is provided. • Assess effectiveness of campaigns and communications.	• Art. 6(1)(a) – Consent for analytics, marketing, and other non-essential cookies and similar technologies. • We rely on legitimate interests only for strictly necessary cookies and do not rely on legitimate interests for non-essential analytics or marketing tags.	Not applicable (analytics and marketing identifiers are not treated as special categories; any health-related inferences are processed only in aggregated or de-identified form).	• Automatically from the browser or device when individuals choose to enable non-essential cookies through the Cookie Preferences Center. • From third-party analytics and advertising providers when	• Web analytics providers. • Advertising and marketing technology providers. • Social media and video platforms where embedded content is enabled. • Email service providers that use web beacons to measure engagement.	• Analytics event data: retained for up to 24 months. • Inference and profile data created for website personalization: retained for the browsing session or de-identified and aggregated within 24 months. • Marketing preferences: retained until you withdraw	• Analytics and marketing providers may be located outside the EEA/UK. • Where personal data is transferred internationally, we implement appropriate safeguards such as Standard Contractual Clauses and the UK International Data Transfer Addendum, together with transfer risk assessments.	• Non-essential tags and cookies do not load until consent is given via Cookiebot. • Consent can be withdrawn at any time via the Cookie Preferences Center; upon withdrawal, non-essential tags are stopped without undue delay. • We honor recognized universal opt-out signals such as Global Privacy

				tags are activated after consent.		consent, unsubscribe, or as required to honor opt-out choices.		Control for sale/sharing and targeted advertising. • We maintain a live cookie registry and do not present an "Unclassified" category to users. • Emails with tracking pixels provide an unsubscribe mechanism; opt-outs are propagated to linked systems.
Approximate geolocation (city or region level) derived from IP address	• Localize content at a regional level (e.g., language or regional pages). • Understand regional interest in our products and services in aggregated form. • Support security and fraud prevention (e.g., anomaly detection).	• Art. 6(1)(f) – Legitimate interests in tailoring content by region and protecting services against misuse. • Art. 6(1)(a) – Consent where location data is processed through analytics or marketing cookies beyond coarse IP-based localization.	Not applicable (approximate geolocation at city/region level is not treated as special category data).	• Automatically from IP address when users visit the website. • From third-party reverse-IP and enrichment services where used for business-to-business insights.	• Hosting, analytics, and security service providers acting as processors. • Corporate affiliates for consolidated regional metrics. • Public authorities where required by law.	• Coarse IP used for session-level localization and security is processed transiently and retained in logs according to the 12-month log schedule. • Aggregated regional analytics is retained for up to 14 months.	• Where approximate geolocation data is transferred outside the EEA/UK, transfers rely on the same safeguards described for logs and analytics (SCCs, UK Addendum, and transfer risk assessments).	• We do not use geofencing to identify, track, or target individuals seeking in-person healthcare services. • We do not use approximate geolocation collected through the website to make medical or diagnostic decisions about individuals.
Website-level inferences (e.g., aggregated interest signals, security risk	• Improve website structure, content, and navigation. • Enhance security monitoring	• Art. 6(1)(f) – Legitimate interests in improving and securing websites	Not treated as special categories. Any health-related interest signals are used only in	• Derived from analytics, logs, and interaction data collected	• Internal teams responsible for product, security, and marketing strategy.	• Inferences that can reasonably be linked to an identifiable	• Aggregated reporting tools may involve transfers outside the EEA/UK with the same	• We do not use website inferences to make automated decisions that produce legal or

indicators)	and anomaly detection. • Support high-level product and content planning (in aggregated form).	and understanding overall user engagement, subject to balancing tests.	de-identified or aggregated form and not to make decisions about identifiable individuals.	through the website. • Derived from aggregated reports provided by service providers.	• Analytics and security providers, acting as processors, that help derive aggregated metrics.	individual are retained no longer than the underlying analytics data (up to 24 months) and are then de-identified or aggregated. • Fully aggregated and de-identified reports may be retained longer for trend analysis.	safeguards (SCCs/UK Addendum and transfer risk assessments).	similarly significant effects on individuals. • We do not build sensitive health profiles for advertising or eligibility decisions based on website browsing.
Feedback and communications (free-text messages, support descriptions, and other content submitted through website forms or email links)	• Respond to questions, requests for information, and support inquiries. • Evaluate and improve products, services, and user experience based on voluntary feedback. • Investigate complaints or security-related reports. • Maintain records necessary for legal, regulatory, or audit purposes.	• Art. 6(1)(f) – Legitimate interests in responding to inquiries, improving services, and maintaining records of interactions. • Art. 6(1)(c) – Compliance with legal obligations where communications relate to regulatory, security, or rights-related matters.	Where individuals voluntarily include information that constitutes special category data (e.g., health status), such data is handled as described for consumer health data and processed only under a lawful basis permitted by Art. 9(2), typically explicit consent (Art. 9(2)(a)).	• Directly from individuals through web forms, email, or other contact mechanisms linked from the website.	• Customer support and CRM service providers acting as processors. • Corporate affiliates and professional advisors involved in handling the inquiry or complaint. • Public authorities or regulators where the communication relates to reportable matters.	• Case-related communications: retained for the life of the inquiry plus approximately 24 months. • Where required for legal defense or compliance, records may be retained longer in accordance with legal limitation periods.	• Communications may be stored or accessed outside the EEA/UK with safeguards as described in ISN-001 (SCCs/UK Addendum and transfer impact assessments).	• Website is not intended for submitting PHI or detailed medical information; individuals are instructed to use secure clinical channels instead. • If sensitive data is submitted unintentionally, it is not used for marketing or profiling and is subject to restricted access.
Call recordings associated with	• Provide quality assurance and training	• Art. 6(1)(f) – Legitimate interests in	Generally, not intended to capture special	• Directly from individuals	• Secure call recording and storage	• Call recordings are typically	• Call recording systems may involve	• Call recording is disclosed at the outset;

website contact (where calls are made to numbers listed on the website and recording is enabled)	for teams handling inquiries. • Maintain a record of conversations related to incident response, security events, or regulatory matters. • Investigate and resolve complaints or disputes.	quality assurance, training, and maintaining records of important interactions. • Art. 6(1)(c) – Compliance with legal obligations where recordings document incidents or regulatory communications.	categories, but where they arise incidentally (e.g., health information shared during a call), such content is handled under the same constraints as consumer health data and only under a permitted Art. 9(2) basis.	participating in recorded calls after notice at the start of the call.	providers acting as processors. • Corporate affiliates and professional advisors involved in the matter documented by the call. • Public authorities or regulators where recordings must be disclosed by law.	retained for approximately 90 days, unless required longer for an active legal, regulatory, or incident investigation, in which case they are retained until the matter is resolved and then deleted.	storage outside the EEA/UK. International transfers use appropriate safeguards such as SCCs/UK Addendum and contractual security controls.	individuals may choose alternative channels if they do not wish to be recorded. • We do not use call recordings for automated decision-making or for targeted advertising.
Financial and transactional data (e.g., payment card details, billing address, transaction identifiers) where purchases or paid registrations occur via the website	• Process payments and complete transactions for events, services, or other offerings available through the website. • Maintain records for accounting, tax, and audit purposes. • Detect and prevent fraud and misuse of payment instruments.	• Art. 6(1)(c) – Compliance with legal obligations related to tax, accounting, and financial reporting. • Art. 6(1)(f) – Legitimate interests in preventing fraud and managing business operations in connection with payments.	Not applicable (financial identifiers are not treated as special category data).	• Directly from individuals when they provide payment details via secure payment forms. • From payment processors that return transaction metadata and status.	• Payment processors and gateways acting as processors. • Financial institutions involved in the transaction. • Corporate affiliates and professional advisors (e.g., auditors) where required. • Public authorities where disclosure is required by tax or financial laws.	• Financial and transactional records are retained for the period required by applicable tax and financial laws, typically 7–10 years depending on jurisdiction.	• Payment processing and related record storage may occur outside the EEA/UK; transfers are safeguarded with appropriate contractual and technical measures (e.g., SCCs/UK Addendum, encryption).	• Payment pages are designed to use secure communication (e.g., TLS) and industry-standard payment security controls. • Payment card data is not used for marketing or profiling.
Consumer health data and other sensitive personal information (voluntarily	• Respond to specific inquiries about our products or services where	• Art. 6(1)(a) – Consent when individuals voluntarily provide	• Directly from individuals who voluntarily include health-relat	• Restricted internal teams responsible for safety,	• Such data is retained only for as long as necessary to address the inquiry	• The website is not intended for submission of PHI;		

provided via website forms, emails, or calls)	individuals choose to disclose information about their health status or related care. • Evaluate safety or product issues raised by healthcare professionals or patients. • Comply with legal obligations and defend legal claims where such data is relevant.	health or other sensitive information for the purpose of receiving a response. • Art. 6(1)(c) – Compliance with legal obligations where reporting or safety follow-up is required. • Art. 6(1)(f) – Legitimate interests in investigating and responding to safety or product questions, balanced against data subject rights. • Art. 9(2)(a) – Explicit consent for processing special categories of data that individuals voluntarily submit. • Other Art. 9(2) bases may apply where required by law (e.g., public interest in the area of public health), and will be identified in product-sp	ed or other sensitive information in website communications. • From healthcare professionals contacting us through channels linked from the website.	regulatory, or product support. • Service providers (e.g., CRM, support tools) with access controls appropriate for sensitive data. • Regulators, public authorities, or legal counsel where legally required or necessary for the establishment, exercise, or defense of legal claims.	or obligation and generally no longer than the underlying contact record (case life plus approximately 24 months), unless a longer period is required by law or for legal defense. • Where feasible, data may be de-identified or minimized as soon as it is no longer needed in identifiable form.	users are instructed to use secure clinical channels instead. • We do not sell consumer health data or sensitive personal information and do not use it for targeted advertising or profiling. • We do not use geofencing to identify, track, or target individuals seeking in-person healthcare services. • Separate consent is obtained where required by law before collecting or sharing consumer health data.		

		ecific notices where relevant.						
Consent records, preference settings, and privacy rights request metadata	• Demonstrate compliance with consent, opt-out, and preference management requirements. • Manage and enforce choices regarding cookies, marketing communications, sale/sharing, and use of sensitive personal information. • Record receipt, handling, and outcome of data subject rights requests and appeals.	• Art. 6(1)(c) – Compliance with legal obligations under GDPR/UK GDPR and applicable state laws concerning consent, opt-outs, and data subject rights. • Art. 6(1)(f) – Legitimate interests in documenting compliance and defending against legal claims.	Not applicable (consent and rights metadata is not treated as special category data).	• Directly from individuals through the Cookie Preferences Center, unsubscribe links, web forms, and email communications. • Automatically from recognized universal opt-out signals (e.g., Global Privacy Control).	• CMP provider (Cookiebot) and related consent logging services acting as processors. • Internal privacy and compliance teams. • Professional advisors and regulators where evidence of compliance is required.	• Consent and preference logs, GPC signals, and rights request records are retained according to legal and audit requirements, typically for the duration of the relationship plus applicable limitation periods.	• Consent and rights-log systems may involve storage outside the EEA/UK with safeguards (SCCs/UK Addendum and transfer impact assessments) as described in ISN-001.	• We honor recognized universal opt-out signals such as Global Privacy Control for sale/sharing and targeted advertising. • We do not discriminate against individuals for exercising their privacy rights. • Records are used solely for compliance and accountability purposes and not for marketing.

For any and all inquiries, please contact our team at privacy@deephealth.com.