

ONLINE PRIVACY NOTICE

LAST UPDATED

29 June 2026

ENTITY

Basecamp Research Ltd

CONTACT

legal@basecamp-research.com

IN THIS NOTICE

- | | | | |
|----|---|----|---|
| 01 | About us | 06 | For how long will we keep your personal data? |
| 02 | What personal data do we process? | 07 | Your rights |
| 03 | How and why do we use your personal data? | 08 | Cookies |
| 04 | With whom do we share your personal data? | 09 | Changes to this Privacy Notice |
| 05 | Where is your personal data processed? | 10 | Contacting us and making a complaint |

01

ABOUT US

This Privacy Notice covers the use of your personal data by Basecamp Research Ltd ("Basecamp Research", "we", "our", or "us").

Basecamp Research Ltd is a private limited company incorporated in England and Wales. We operate two distinct online services:

- **Corporate website:** available at <https://www.basecamp-research.com> (the "Site"), providing information about our company, biodiscovery services, and biological data products. Basecamp acts as a data controller in respect of personal data processed through the Site.
- **EDEN MCP service:** available at <https://mcp-public.basecamp-research.com> (the "EDEN MCP Service"), an authenticated Model Context Protocol (MCP) API providing research tools for biological sequence generation, analysis and dataset handling. Basecamp may act as either a data controller or a data processor in respect of personal data processed through the EDEN MCP Service, depending on the context in which the EDEN MCP Service is used.

Because these two services process different categories of personal data through different technical means, this Privacy Notice addresses them separately where relevant. References to "our services" cover both unless stated otherwise.

If you have any questions about this Privacy Notice, please contact us at legal@basecamp-research.com.

02

WHAT PERSONAL DATA DO WE PROCESS?

2.1 Corporate website

When you interact with the corporate website, we collect:

- **Contact enquiries:** any information you submit via our 'Contact Us' form, by email, or in person, including the content of your message.
- **Business contacts:** your name, organization name and address, job title, email address, telephone number, and any other information relevant to our business relationship with you.
- **Job applicants:** details provided as part of a job application, including your CV, employment history, qualifications, references, and — where legally required — immigration status, right-to-work documentation (e.g. passport, visa, biometric residence permit), and other visa or immigration-related information.
- **Technical Data:** Internet Protocol (IP) address, browser type and version, time zone and location settings, browser plug-in types and versions, operating system and platform, and other device information.
- **Usage Data:** information about how you use the Site, including pages visited, time spent, and frequency of visits.
- **Log Data:** server log files generated when you visit the Site, which may include your IP address, browser type, pages visited, and timestamps.
- **Aggregated and anonymized data:** statistical and summary data compiled from multiple users for analytics and reporting. Where data is truly anonymized and cannot identify an individual, it falls outside the scope of this Privacy Notice.

2.2 EDEN MCP Service

The EDEN MCP Service is provided as an authenticated API, with access restricted to authenticated users:

- **Registered Users:** life sciences researchers who register for the EDEN MCP Service directly through open registration.
- **Indirect Users:** individuals who access the EDEN MCP Service indirectly through Anthropic's "Claude Bioscience Beta" integration and may have no direct contractual relationship with us.

- **Internal Users:** members of staff at Basecamp Research and at Anthropic who access the EDEN MCP Service in connection with the provision, administration, or support of the service.

Access requires you to sign in using a Google or Microsoft account. When you do so, you are presented with our Terms of Service and a link to this Privacy Notice. If you are located in a jurisdiction in which acceptance of a privacy policy can constitute consent to the processing described below, your use of the service constitutes your explicit consent to such processing. If you are located in the UK or the EEA, this Privacy Notice is provided for informational purposes only.

When you use the EDEN MCP Service, we collect and process some or all of the following categories of personal data:

(a) Account and authentication information

- **Identity data from your Google or Microsoft account:** when you authenticate, we receive your full name, email address, and a unique account identifier from your identity provider. We do not receive or store your Google or Microsoft password.
- **IP address:** collected at the point of authentication and during active sessions for security monitoring, access control, service integrity and fraud prevention purposes.
- **Session tokens:** issued by our authentication provider upon sign-in to maintain your authenticated session.

(b) Biological and scientific data

- **Biological sequence data:** nucleotide or amino acid sequences, or other biological inputs that you submit to the service for analysis, including nucleotide or genomic sequences, strain-specific sequences, and protein or peptide sequences.
- **Uploaded datasets:** files or structured data you upload to the EDEN MCP Service for processing or storage, including supporting documents such as human microbiology reports, clinical materials, or other documents that may identify, or contribute to the identification of, an individual.
- **Dataset metadata:** descriptive information associated with your uploaded data, such as file names, formats, sizes, upload timestamps, and any labels or annotations you provide in connection with uploaded data.

- **Service-generated outputs:** results, analyses, predictions, annotations, and other outputs produced by the service in response to your inputs. These outputs may incorporate or reference your submitted data and may be retained to support service delivery and quality assurance.

(c) Technical usage records

- **API usage logs:** records of which tools and endpoints you accessed, the frequency and timing of requests, request parameters (which may include submitted data), and response metadata.
- **Performance and error data:** technical data about service performance, errors, and system events, used for monitoring, debugging, and improving the service.

We wish to be transparent about the following: (i) submitted scientific data, including sequences and datasets, may be retained on our systems and those of our service providers for the periods described in Section 6; (ii) not all data can be deleted immediately or entirely through self-service functionality — if you wish to request deletion, please contact us as set out in Section 10; and (iii) aggregated or derived data generated from your inputs may be retained in anonymized form after your individual data is deleted; and (iv) the sequences you submit, the outputs generated by the service, and your identity and usage data are subject to biosecurity screening, logging, and potential reporting to authorities as described in Section 3.7.

2.3 Personal data we receive from third parties

We may receive personal data about you from third parties in the following circumstances:

- Your employer designates you as their contact person and passes your details to us.
- We collect publicly available profile information from professional social media platforms such as LinkedIn in connection with our business activities.
- We obtain business contact information from third-party B2B data providers for outreach and marketing purposes. Where we do so, we take steps to ensure those providers have a lawful basis for sharing your information with us.
- We use third-party background check providers as part of our due diligence processes where legally permitted and necessary.
- For EDEN MCP users, we receive identity data from your chosen identity provider (Google or Microsoft) as described in Section 2.2(a) above.

Where we need to collect personal data by law or under the terms of a contract, and you fail to provide it when requested, we may be unable to perform that contract or progress your application. We will notify you if this is the case.

If you provide us with personal data – including special category and criminal offence data – about one or more third parties in connection with the EDEN MCP Service, you are responsible for ensuring that a lawful basis exists for sharing that personal data with us for the processing of each third party's personal data for the purposes set out in this Privacy Notice.

03

HOW AND WHY DO WE USE YOUR PERSONAL DATA?

We will only use your personal data where the law permits us to do so. The legal bases on which we rely are:

- **Contract performance:** where processing is necessary to perform a contract we have with you or your organization, or to take steps at your request prior to entering into a contract.
- **Legitimate interests:** where processing is necessary for our legitimate business interests (or those of a third party), provided those interests are not overridden by your rights and interests. You may contact us for further information about our legitimate interests assessment.
- **Legal obligation:** where processing is necessary to comply with a legal or regulatory obligation.
- **Consent:** where you have given us your explicit consent to process your data for a specific purpose.
- **Vital interests:** in exceptional circumstances, where processing is necessary to protect the vital interests of you or another person.

We use your personal data for the following specific purposes:

3.1 Business relationship management

If you are a business contact, we will use your personal data to: communicate with you about our services; respond to enquiries or concerns; manage our business relationship; conduct administrative tasks; and, where applicable, prevent fraud. We do this on the basis of our legitimate business interests.

3.2 EDEN MCP Service delivery

We use your account, authentication, scientific data, and usage information to: verify your identity and maintain your authenticated session; provide the analysis tools and dataset handling functionality you request; generate, store, and return service outputs; and ensure the security and integrity of the service. This processing is necessary to perform our contract with you and for our legitimate interests in providing and optimizing the Service.

3.3 Service monitoring, security, and improvement

We use technical usage records and log data from both the Site and the EDEN MCP Service to: operate, maintain, and improve our services; monitor and analyze usage patterns; detect and prevent unauthorised access, fraud, and security incidents; and ensure the reliability and performance of our systems. We do this on the basis of our legitimate interests in operating secure and effective services.

3.4 Visitor management

For visitors to our offices, to maintain the safety and security of our premises and to meet our health and safety legal obligations.

3.5 Legal compliance

To comply with applicable legal and regulatory obligations, to respond to lawful requests from public authorities, and to establish, exercise, or defend legal claims.

3.6 Recruitment and immigration

To process job applications, conduct pre-employment checks, and facilitate visa applications, renewals, and immigration compliance with the relevant authorities and government bodies.

3.7 Biosecurity screening, monitoring, and reporting

The EDEN MCP Service generates and analyzes biological sequence data, including nucleic acid and amino acid sequences. To detect and prevent misuse of the service — including use that could contribute to the development of biological or other weapons — we operate biosecurity controls. This involves screening the sequences you submit and the outputs the service generates against curated reference databases, applying identity- and legitimacy-verification (know-your-customer) checks, conducting follow-up review of flagged activity, and filtering,

withholding, or refusing requests or outputs that raise biosecurity concerns. Our controls are informed by recognized nucleic acid synthesis screening norms, adapted for a computational service.

Where our screening or review identifies activity that we reasonably believe may be unlawful, may indicate an intent to cause harm, or may relate to the development of weapons, we may report the activity — together with relevant logs, sequences, and identity and affiliation information — to relevant law enforcement, biosecurity, public-health, regulatory, or export-control authorities, and to other screening providers or coordinating bodies. We may do so without prior notice to you where notice would be unlawful or would prejudice an investigation.

We carry out this processing on the basis of our legitimate interests (and the public interest) in preventing the misuse of biological research tools and in protecting biosecurity and public health, and in order to comply with our legal obligations; where relevant, we may also rely on the protection of the vital interests of an individual. We do not rely on your consent for biosecurity screening, logging, or reporting, and withdrawing any consent you have given for other processing does not affect these activities. You may contact us for further information about the relevant legitimate interests assessment.

3.8 Special category and criminal offence data

Many biological sequences processed by the EDEN MCP Service are scientific research data and will not, in themselves, identify a living individual. However, genomic sequences, clinical data, health information, human microbiology reports, service-generated reports, or other information submitted to or generated through the EDEN MCP Service may relate to an identified or identifiable living individual, and where such information includes genetic data, data concerning health or other special category data, we will process it only where both a lawful basis under Article 6 of the General Data Protection Regulation (“GDPR”) and United Kingdom GDPR (“UK GDPR”) and a separate condition under Article 9 of the GDPR and UK GDPR are satisfied. In particular, for purposes of the UK GDPR, we will rely on the substantial public interest condition (Article 9(2)(g)), read with the relevant condition in Schedule 1 to the Data Protection Act 2018, in respect of this processing. Where our biosecurity processing involves information about actual or suspected criminal offences, we process that information in reliance on the conditions for criminal offence data under the Data Protection Act 2018.

04

WITH WHOM DO WE
SHARE YOUR
PERSONAL DATA?

We will share your personal data only where necessary and only with the following categories of recipients:

- **Internal staff:** employees and contractors of Basecamp Research who need access to your information to carry out their duties in line with the purposes set out in this Privacy Notice.
- **Professional advisers:** our legal, financial, and accounting advisers where they require your information to provide advice to us.
- **Group companies and affiliates:** other entities within our corporate group, where necessary for the purposes described in this Privacy Notice.
- **Infrastructure and service providers:** third parties we engage to support the delivery and operation of our services, including:
 - **Authentication:** Auth0 (Okta), Google, and Microsoft provide authentication services for the EDEN MCP Service. These providers receive your identity data as part of the sign-in flow.
 - **Cloud hosting and compute:** Amazon Web Services (AWS) provides the hosting and computational infrastructure on which the EDEN MCP Service and associated data are processed and stored.
 - website hosting, maintenance, and infrastructure providers;
 - customer relationship management (CRM) and data storage platforms;
 - form processing and communication tools;
 - network security, fraud prevention, spam detection, and site protection services;
 - monitoring, logging, and performance analytics platforms;
 - background check and due diligence providers.
- **Corporate transactions:** if we undergo a merger, acquisition, restructuring, or sale of assets, your information may be disclosed to the relevant counterparty as part of due diligence. If the transaction completes, your information may be transferred to the acquiring entity, subject to an equivalent level of protection.
- **Regulatory and government bodies:** immigration authorities, consulates, embassies, visa authorities, and related service providers to the extent required under applicable law; and law enforcement agencies or other public authorities where required by law or court order.

- **Biosecurity and screening recipients:** where our biosecurity screening or review identifies concerning activity, we may disclose relevant records (including logs, sequences, and identity and affiliation information) to law enforcement, biosecurity, public-health, regulatory, and export-control authorities, and to other nucleic acid synthesis screening providers or coordinating bodies, as described in Section 3.7. This may include proactive disclosure that is not required by a court order.
- **Third-party linked sites:** our Site may contain links to third-party websites. We do not control those sites and are not responsible for their privacy practices. We encourage you to read the privacy notice of every website you visit.

We require all third parties to respect the security of your personal data and to treat it in accordance with applicable data protection law. We do not permit our service providers to use your personal data for their own purposes.

05

WHERE IS YOUR PERSONAL DATA PROCESSED?

The location of processing differs between our two services. We set out below the principal processing locations for each.

5.1 Corporate website

Data submitted through the corporate website is stored electronically on secure servers primarily located within the UK and the EEA, and any physical records are held at our UK business premises.

5.2 EDEN MCP Service

The EDEN MCP Service involves processing across multiple infrastructure providers and regions, as follows:

- **Amazon Web Services (AWS) — Cloud hosting and compute:** data is processed and stored in the following AWS regions: eu-west-2 (London, UK) as our primary region; and us-east-1 and us-east-2 (Northern Virginia and Ohio, USA) for certain computational workloads, redundancy, or service components. Data processed in US regions is subject to the international transfer safeguards described below.
- **Auth0 (Okta) — Authentication:** authentication data (including your identity credentials and session tokens) is processed within Auth0's UK region deployment.

- **Google — Identity provider:** if you sign in using a Google account, your authentication request is processed by Google. Google operates global infrastructure and may process data across multiple jurisdictions. Google's processing is governed by Google's own privacy policy and, where applicable, Google's data processing terms.
- **Microsoft — Identity provider:** if you sign in using a Microsoft account, your authentication request is processed by Microsoft. Microsoft operates global infrastructure and may process data across multiple jurisdictions. Microsoft's processing is governed by Microsoft's own privacy policy and, where applicable, Microsoft's data processing terms.

5.3 International transfers and safeguards

Where personal data is transferred to countries outside the UK or EEA that do not benefit from an adequacy decision, we ensure that appropriate safeguards are in place. In particular:

- Transfers to AWS US regions are governed by the AWS Data Processing Addendum, which incorporates the UK International Data Transfer Addendum (IDTA) and/or EU Standard Contractual Clauses (SCCs) as applicable.
- Transfers via Google and Microsoft as identity providers are governed by those providers' respective data processing agreements, which include SCCs or equivalent transfer mechanisms.
- We conduct transfer impact assessments where required and will not transfer personal data internationally unless we are satisfied that adequate protections are in place.

Please contact us if you would like further information about the specific safeguards applicable to any particular transfer.

While we take all reasonable steps to protect your personal data, we cannot guarantee the security of data transmitted over the internet. Any such transmission is at your own risk. Once we receive your data, we apply strict technical and organizational security measures to prevent unauthorised access, loss, or disclosure.

06

FOR HOW LONG WILL WE KEEP YOUR PERSONAL

DATA?
BEYOND KNOWN BIOLOGY™

We retain personal data only for as long as is reasonably necessary to fulfill the purposes for which it was collected, including satisfying any legal, regulatory, accounting, or reporting obligations.

In determining the appropriate retention period, we consider:

- the amount, nature, and sensitivity of the personal data;
- the potential risk of harm from unauthorised use or disclosure;
- the purposes for which we process the data and whether we can achieve those purposes through other means; and
- applicable legal and regulatory requirements.

As a general guide, our standard retention periods are:

Corporate website data

- **Social media profile data:** up to 1 year from the date of collection.
- **Job applicants:** up to 1 year from the end of the recruitment process, unless: (a) you have provided consent to be retained for future opportunities; (b) a longer period is required by law; or (c) the information is necessary for legal proceedings or compliance purposes.
- **Business contact information:** for the duration of our business relationship and up to 5 years thereafter, or as required by applicable law.
- **Contact form and general correspondence:** up to 2 years from submission or last correspondence, unless the information is required for ongoing legal or business purposes.
- **Website technical and log data:** typically up to 12 months from collection, unless required for security investigations or legal proceedings.

EDEN MCP Service data

- **Account and authentication data:** retained for the duration of your active account and for up to 2 years following account closure or last authenticated access, to support audit, security, and legal compliance purposes.
- **Biological sequence data and uploaded datasets:** retained for the duration of your use of the service and for a reasonable period thereafter (typically up to 2 years) to support service delivery, unless you request earlier deletion in accordance with Section 10. Please note that deletion requests are processed manually and may not result in immediate or complete removal from all backup or archival systems.
- **Dataset metadata and service-generated outputs:** retained for the same period as the underlying data to which they relate, or for up to 2 years following the last relevant activity, whichever is later.

- **API usage and technical logs:** typically retained for up to 12 months from the date of generation, unless retained for longer for security investigation, legal proceedings, or regulatory compliance purposes.
- **Biosecurity screening and flagged-activity records:** records relating to activity that has been flagged, refused, escalated, or reported for biosecurity reasons, and records of any report made to authorities, are retained for up to 8 years from the date of the relevant activity (consistent with record-retention periods reflected in nucleic acid synthesis screening norms such as the IGSC Harmonized Screening Protocol), or for longer where required by law or necessary for the establishment, exercise, or defense of legal claims.

We will securely delete or anonymize your personal data when it is no longer needed. In some circumstances we may anonymize data for research or statistical purposes, in which case that anonymized data may be retained and used indefinitely without further notice to you.

07

YOUR RIGHTS

Under applicable data protection law (including the UK GDPR and Data Protection Act 2018), you have the following rights in relation to your personal data:

- **Right to be informed:** to receive clear, transparent, and easily understandable information about how we use your data — which this Privacy Notice provides.
- **Right of access:** to obtain a copy of your personal data and certain information about how we process it (commonly known as a 'Subject Access Request').
- **Right to rectification:** to have inaccurate or incomplete personal data corrected.
- **Right to erasure ('right to be forgotten'):** to request deletion of your personal data where there is no compelling reason for us to continue processing it. Note that this right is not absolute and is subject to certain exceptions. For EDEN MCP users, erasure requests in relation to scientific data, outputs, and logs are handled manually — please contact us using the details in Section 10. We will action valid requests as promptly as practicable, but complete removal from all backup and archival systems may take additional time.

- **Right to restrict processing:** to request that we suspend use of your personal data in certain circumstances, for example while accuracy is being verified.
- **Right to data portability:** to receive your personal data in a structured, commonly used, and machine-readable format, and to have it transferred to another controller in certain circumstances.
- **Right to object:** to object to processing of your personal data based on our legitimate interests, including for direct marketing purposes. Where you object to direct marketing, we will stop processing your data for that purpose immediately and without exception.
- **Right to withdraw consent:** where processing is based on your consent (including for EDEN MCP users), to withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out prior to withdrawal, and will not automatically result in deletion of data already processed.
- **Rights in relation to automated decision-making:** not to be subject to a decision based solely on automated processing (including profiling) that produces legal or similarly significant effects on you, unless certain conditions apply.

Some of these rights are limited where your data is processed for biosecurity purposes (see Section 3.7). In particular, we may be unable to comply fully with a request for erasure or restriction where we need to retain records for biosecurity, to comply with a legal obligation, or for the establishment, exercise, or defense of legal claims (Article 17³ UK GDPR). Where you object to processing based on our legitimate interests (Article 21), we may continue where we can demonstrate compelling legitimate grounds, including the prevention of serious harm. We may also withhold information about a specific screening decision or a disclosure to authorities where providing it would prejudice the prevention or detection of crime or an investigation.

To exercise any of these rights, please contact us at legal@basecamp-research.com. We will respond to your request within one month as required by law, though we may extend this period by a further two months in complex cases and will notify you accordingly. We will not charge a fee for handling your request unless it is manifestly unfounded or excessive.

We may need to verify your identity before responding to certain requests. We will take reasonable steps to do so in a way that does not unduly burden you.

08

COOKIES

We use cookies and similar tracking technologies on the Site. Cookies are small text files placed on your device that help us maintain your connection to the Site and improve your experience. The EDEN MCP Service uses session tokens issued by Auth0 to maintain authenticated sessions; these function similarly to cookies in a browser context. For full details of the cookies used on the Site and how to manage your preferences, please see our Cookie Policy at <https://www.basecamp-research.com/cookie-policy>.

09

CHANGES TO THIS PRIVACY NOTICE

We may update this Privacy Notice from time to time to reflect changes in our practices, legal requirements, or operational circumstances. Where changes are material, we will take reasonable steps to notify you (for example, by posting a prominent notice on our Site, updating the notice presented at EDEN MCP sign-in, or, where appropriate, contacting you directly).

This Privacy Notice was last updated on **29 June 2026**. We encourage you to review this Privacy Notice periodically.

10

CONTACTING US AND MAKING A COMPLAINT

10.1 General privacy enquiries

If you have any questions, concerns, or requests regarding this Privacy Notice or our data processing activities — including requests relating to your EDEN MCP Service data — please contact us in the first instance by email at legal@basecamp-research.com. Please provide as much detail as possible, including the service concerned, relevant dates, individuals involved, and any supporting documents.

We will endeavour to acknowledge your enquiry promptly and respond fully within a reasonable timeframe.

10.2 Escalation

If you are not satisfied with our initial response, you may escalate your concern in writing to legal@basecamp-research.com or by post to:

FAO: Head of Legal

Basecamp Research Ltd
Unit 315, Clerkenwell Workshops
27 Clerkenwell Close
London, England, EC1R 0AT
United Kingdom

We will investigate your complaint and respond within a reasonable timeframe.

10.3 Right to complain to a supervisory authority

If you remain unsatisfied with our response, you have the right to lodge a complaint with the relevant data protection supervisory authority. In the UK, this is the Information Commissioner's Office (ICO). You can find more information at www.ico.org.uk. The ICO can be contacted by telephone on 0303 123 1113.

We would, however, appreciate the opportunity to address your concerns before you approach the ICO, and encourage you to contact us in the first instance.