Romi

Document Management

Organisation: Romi

Issue Date: Nov 20, 2026

Document Owner: Vlad Bacila (DPO)

Privacy Notice

This Privacy Notice gives you information about how Neuro Notion App Limited ("Romi", "we", "us" or "our") collects and uses your personal data through your use of our mobile application and website, and when you communicate with us in any way, including any data you may provide when you sign up and use our services.

Who we are and how to contact us

Neuro Notion App Limited is the controller and responsible for your personal data. We are a company registered in England and Wales with company number 15345630, with our registered office at 124 City Road, London, England, EC1V 2NX.

If you would like to contact us about anything in this Privacy Notice, or if you have any questions about how we use your information or would like to exercise any of your data subject rights, please contact our Data Protection Officer:

Vlad Claudiu Bacila, Data Protection Officer

Email: vlad@romiadhd.com

Important notice: how you use our app affects your rights

Your data rights and our legal obligations depend on how you joined our service. Please read the description that applies to you:

Direct Users

If you signed up independently (for example, via the App Store or directly through our website), Neuro Notion App Limited is the Data Controller of your personal data and this Privacy Notice applies in full.

Clinic Patients (where a Data Processing Agreement is in place)

If you were invited to use our app by a healthcare provider, clinic, or hospital ("Healthcare Provider") AND Romi has a formal Data Processing Agreement (DPA) in place with that Healthcare Provider that explicitly transfers data controllership, your Healthcare Provider is the Data Controller of your health data. In that context, Neuro Notion App Limited acts as a Data Processor and processes your data strictly in accordance with your Healthcare Provider's instructions and our contract with them.

Important: Even if you use our app in connection with a healthcare organisation, Romi remains the Data Controller unless a formal DPA has been executed between us and that organisation that explicitly transfers data controllership. If no such agreement is in place, this Privacy Notice applies in full and Neuro Notion App Limited is the controller of your personal data.

The types of personal data we collect

Personal data means any information about an individual from which that person can be identified. We may collect, use, store and transfer different kinds of personal data about you, grouped as follows:

Identity Data: email address, first name and last name.

Contact Data: billing address, email address and telephone numbers.

Transaction Data: details about payments to and from you and other details of products and services you have purchased from us.

Technical Data: internet protocol (IP) address, your login data, browser type and version, time zone setting and location, device ID and other technology on the devices you use to access our app and website.

Profile Data: your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

Usage Data: information about how you interact with and use our app, products and services, including task and routine data, journal entries, mood tracking data, mental health insights, voice transcriptions, and goal and progress information.

Marketing and Communications Data: your preferences in receiving marketing from us and your communication preferences.

Health Data: any data about your health, ADHD symptoms, mood, or wellbeing that you share with us when you express interest in, sign up for, and/or use our services. This is special category data under UK GDPR and we handle it with the highest level of care and only with your explicit consent.

We also collect, use and share anonymised aggregated data such as statistical or demographic data which is not personal data as it does not directly or indirectly reveal your identity. For example, we may use this anonymised data to help us build evidence to justify formal clinical trials and feasibility studies, for internal research and product development, or for future publications.

1.0 How is your personal data collected?

We use different methods to collect data from and about you, including through:

Your interactions with us.

You may give us your personal data by signing up to use the mobile app, filling in online forms, or by corresponding with us by phone, email or otherwise. This includes personal data, including special category health data, that you provide when you:

- create an account to use the Romi mobile app;
- sign in to use the Romi mobile app;
- subscribe to our newsletters or publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us feedback or contact us.

Automated technologies or interactions.

As you interact with our website, we will automatically collect Technical Data about your equipment and usage patterns. Please see section 2.6 for details of our use of cookies on our website. We do not collect cookies from users within the mobile app itself.

Third parties.

We may receive personal data about you from Healthcare Providers where a formal Data Processing Agreement is in place. We may also receive data from analytics and technical service providers as described in section 3.0 below.

2.0 How we use your personal data

2.1 Legal basis

The law requires us to have a legal basis for collecting and using your personal data. We rely on one or more of the following legal bases:

Performance of a contract with you: Where we need to perform the contract we are about to enter into or have entered into with you.

Legitimate interests: We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience. We make sure we consider and balance any potential impact on you and your rights before we process your personal data for our legitimate interests.

Legal obligation: We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Consent: We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose. For health data, we always require your explicit consent.

2.2 Purposes for which we will use your personal data

The table below describes how we plan to use the various categories of your personal data, and which legal bases we rely on to do so.

Purpose / Use	Type of data	Legal basis
To register you as a new user	(a) Identity (b) Contact	Performance of a contract with you
To identify payments you have made to us, any refunds due, and to identify products or services you have purchased	Transaction Data	Performance of a contract with you
To process and deliver our services to you, including providing accurate educational and supportive materials	(a) Identity (b) Health	(a) Performance of a contract with you (b) Explicit Consent for Health Data
To manage our relationship with you, including notifying you about changes to our terms or Privacy Notice, and dealing with your requests, complaints and queries	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Legal obligation (c) Legitimate interests (keeping records updated)
To enable you to complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Legitimate interests (to study how users use our products) (b) Consent
To administer and protect our business and mobile app (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting)	(a) Identity (b) Contact (c) Technical	(a) Legitimate interests (running our business, IT services, network security, fraud prevention) (b) Legal obligation
To use data analytics to improve our app, products/services, and customer relationships, and to measure effectiveness of our communications	(a) Technical (b) Usage	Legitimate interests (to define types of customers, keep our app updated and relevant, develop our business)
To send you relevant marketing communications and make personalised recommendations based on your profile	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Consent, having obtained your prior consent to receiving direct marketing
To carry out market research through your voluntary participation in surveys	(a) Identity (b) Usage	Legitimate interests (to study how users use our products and to help us improve and develop our products and services)
To provide you with a method of recording and reporting your symptoms, mood and ADHD-related experiences whilst using our services	(a) Identity (b) Contact (c) Profile (d) Health	(a) Performance of a contract with you (b) Explicit Consent for Health Data (Article 9(2)(a) UK GDPR)
To provide you with the most relevant educational and informational content	(a) Identity (b) Contact (c) Profile (d) Health	(a) Performance of a contract with you (b) Explicit Consent for Health Data (Article 9(2)(a) UK GDPR)
To share your own self-reported entries with your Healthcare Provider, exactly as you entered them, along with group figures across the clinic's patients, where you joined Romi through them and consent (Clinic Patients only)	(a) Identity (b) Health (c) Usage (d) Clinic Reference Number	(a) Where a DPA is in place: performance of contract with Healthcare Provider and Provision of Health Care (Article 9(2)(h) UK GDPR) (b) Where no DPA is in place: your Explicit Consent (Article 9(2)(a) UK GDPR)

2.2.1 Neuro Notion App Limited **as a data processor**

Where Neuro Notion App Limited has entered into a formal Data Processing Agreement (DPA) with a Healthcare Provider, we act as a data processor in respect of patient data. This means we process that patient data only according to the instructions of the data controller, which is the Healthcare Provider (such as a clinic, NHS trust, or private practice). They maintain overall responsibility for patient data and the circumstances of processing.

In those cases, Neuro Notion App Limited **processes data under the Healthcare Provider's instructions and the legal basis they determine. In most cases the Healthcare Provider will rely on:**

Article 6(1)(e) UK GDPR: processing necessary to provide a service which is in the public interest; and

Article 9(2)(h) UK GDPR: processing of health information necessary for the provision of health treatment.

Where Neuro Notion App Limited is acting as a data processor for a Healthcare Provider, to find out more about how your data is protected or to exercise your rights under data protection law, you should contact your Healthcare Provider directly in the first instance.

Reporting to your clinic: Where you join Romi through your clinic and consent, we share your own self-reported entries with your clinic, exactly as you entered them and without summarising them: your check-in ratings, the moods you picked, your questionnaire answers and totals, the regulation exercises you completed and counts of your tasks. Your clinic never receives your conversations with Romi, your journal, your notes or your task titles. Your individual entries are only available in the Romi clinic dashboard, which needs a secure sign-in, and in password-protected files your clinic downloads from it. Your clinic finds your entries using its own patient number for you, not your name. Your clinic also sees group figures across its patients who share their data. Group figures are shown in the dashboard and also sent as password-protected PDF reports, and are only shown when at least 7 patients are included. Data is sent over encrypted connections. If your clinic uses Cliniko, Semble or another electronic patient record system, we also send your entries into your record in the clinic's system, so they sit alongside the rest of your care. Your clinic links your Romi account to your record using its own patient number, and we only send to that record. Romi does not monitor your entries or alert your clinic, and your clinic may not look at them between appointments. If you withdraw your consent, we stop sharing. Where we have a data processing agreement with your clinic, your clinic is the data controller for your data and we are its processor. Otherwise we are the data controller and share your individual data with your clinic only with your explicit consent.

2.3 Direct marketing

We may use your personal data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt out of receiving any or all of these communications from us by following the unsubscribe link or instructions provided in any email we send, or by contacting us at vlad@romiadhd.com.

2.4 Third-party marketing

We will get your express consent before we share your personal data with any third party for their own direct marketing purposes.

2.5 Opting out of marketing

You can ask us to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you or by contacting us at vlad@romiadhd.com. If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes.

2.6 Cookies

Our website (www.romiadhd.com) uses a small amount of strictly necessary browser storage. It also uses PostHog analytics cookies to understand how visitors use the site so we can improve it. We do not use cookies within our mobile app, and we do not use advertising cookies, pixels or web beacons.

When you first visit, a small notice tells you about our analytics and lets you opt out. UK law allows analytics cookies used only to improve a website without asking for consent first, as long as you can opt out at any time. We also use Vercel Analytics, which does not use cookies.

- **Strictly necessary storage:** remembers your analytics choice and keeps the site working.
- **Analytics cookies (PostHog, unless you opt out):** tell us which pages are visited and how the site is used, so we can improve it.

To opt out, or to turn analytics back on, use the Cookie settings link at the bottom of any page on our website, or contact us at vlad@romiadhd.com. Our Cookies Policy has more detail.

3.0 Disclosures of your personal data

We do not sell, rent or trade your personal data to advertisers, data brokers or pharmaceutical companies. We may share your personal data where necessary with the following categories of third parties for the purposes described in this Privacy Notice. We have Data Processing Agreements in place with all third-party service providers and we only permit them to process your personal data for specified purposes and in accordance with our instructions.

3.1 Third-party service providers

Provider	Location	Purpose	Key safeguards
Supabase, Inc.	UK (AWS, London)	Database hosting, authentication, data storage	SOC 2 Type II, GDPR compliant, AES-256 encryption at rest, Row Level Security
GCP (Google Cloud Platform)	EU / UK	Cloud infrastructure and identity provider	ISO 27001 certified, GDPR compliant, encrypted in transit and at rest
Vercel, Inc.	USA / EU	Web hosting and front-end deployment	GDPR compliant, encrypted in transit via TLS
Cloudflare, Inc.	USA / EU	CDN, DDoS protection, network security, and storage of security logs (EU, kept 12 months, deleted after 24 months)	GDPR compliant, SOC 2 Type II certified
ElevenLabs	USA / EU	Voice conversations with Romi: speech-to-text, the voice companion and voice synthesis	GDPR compliant, encrypted in transit and at rest
OpenAI and Anthropic	USA	AI language model processing	GDPR compliant, Standard Contractual Clauses, data not used for model training under API terms
Mem0	USA	AI memory layer. Holds memory notes under a pseudonymous user ID, with no name or email.	A data processing agreement with UK International Data Transfer Addendum terms covers the transfer. Encrypted in transit and at rest.
Stripe, Inc.	USA	Secure payment processing and subscription management	PCI DSS Level 1 certified. We never store or access payment card information.
PostHog, Inc.	USA / EU	Anonymised usage analytics and product improvement	GDPR compliant. No user IDs, email addresses or personal content transmitted.
Crisp IM SAS	EU	Real-time customer support and communication	GDPR compliant, encrypted conversations. Disable via your preferences at any time.
Firebase (Google LLC)	USA / EU	Push notifications to iOS and Android devices	Encrypted transmission. Tokens stored securely. Disable notifications via your device settings.
Resend, Inc.	EU (Ireland)	Transactional email delivery including account verification	GDPR compliant. TLS-encrypted. No tracking pixels or email open tracking.
Mooseend	EU	Email marketing communications	GDPR compliant. Used only where you have given consent to receive marketing communications.
Healthcare Providers (Clinic Patients who consent)	UK / EEA	The patient's own self-reported entries, exactly as entered, and group figures across the clinic's patients (Clinic Patients only), including into the clinic's own patient record system (Cliniko, Semble or a bespoke EPR) where the clinic uses one	Shared only where the patient joined Romi through the clinic and consents. Individual entries only in the clinic dashboard with secure sign-in, and in password-protected files the clinic downloads from it. Group figures also sent as password-protected PDF reports. Encrypted connections. Group figures only shown for 7 or more patients. No conversation transcripts or content. Where a DPA is in place the clinic is the controller (Article 9(2)(h) UK GDPR); otherwise shared only with the patient's explicit consent.

3.2 Business transactions

If Neuro Notion App Limited is involved in a merger, acquisition or asset sale, your personal data may be transferred. We will provide notice before your personal data is transferred and becomes subject to a different Privacy Notice.

3.3 Law enforcement

Under certain circumstances, we may be required to disclose your personal data if required to do so by law or in response to valid requests by public authorities (for example, a court or a government agency).

3.4 Other legal requirements

We may disclose your personal data in the good faith belief that such action is necessary to:

- comply with a legal obligation;
- protect and defend the rights or property of Neuro Notion App Limited
- prevent or investigate possible wrongdoing in connection with the service;
- protect the personal safety of users of the service or the public; or
- protect against legal liability.

4.0 International transfers

We may transfer your personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside the UK or EEA to countries which have laws that do not provide the same level of data protection as UK or EU law.

Some of our directors may access personal data from outside the UK, including from the Philippines, to run and support Romi. This is access by our own staff, not a transfer to another organisation, and it uses the same protections as all staff access: multi-factor authentication, encrypted devices, no local copies of personal data, and logged access.

Whenever we transfer your personal data out of the UK or EEA, we ensure a similar degree of protection is afforded to it by ensuring that one or more of the following safeguards are in place:

We will only transfer your personal data to countries that have been deemed by the UK or EU to provide an adequate level of protection; or

We use specific standard contractual clauses (SCCs) approved for use in the UK and/or EEA, which give the transferred personal data the same protection as it has in the UK or EEA.

To obtain a copy of these contractual safeguards, please contact us at vlad@romiadhd.com.

5.0 Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and are subject to a duty of confidentiality.

5.1 People

Training: All staff receive regular appropriate training on data protection and security.

Minimised access: Your personal data, including Health Data, can only be accessed on a strictly need-to-know basis by our Chief Technology Officer, as and when necessary.

Security expertise: We utilise qualified security professionals with recognised experience in technical security architecture and governance, risk and compliance.

5.2 Cyber resiliency, business continuity and disaster recovery

We utilise secure and resilient cloud infrastructure (Supabase on AWS in London, UK, and Google Cloud Platform) which ensures servers are always patched and up to date. Web servers store no sensitive information; this is retrieved from an AES-256 encrypted database hosted by Supabase on AWS in London, UK. Supabase takes daily backups with point-in-time recovery, kept for 7 days. A weekly encrypted copy is kept outside Supabase for 90 days. Automated tests are performed internally across the codebase on every commit. We commit to undertaking regular third-party security audits with certified security auditors, including annual penetration tests.

5.3 Technology

We adopt principles of Secure by Design, including:

- Architecture in line with industry standards, including role-based access controls.
- REST APIs with authentication and authorisation to ensure data minimisation and prevent unauthorised access.
- Strong password validation, with passwords stored hashed using bcrypt with salting.
- Encryption in transit using TLS 1.2 or higher and secure ciphers; encryption at rest using AES-256.
- Data hosted by Supabase on AWS in London, UK.
- Logical separation of production and development environments, including isolated databases.
- Automated tests and Dependabot alerts on every change, and code review before merging.
- Annual manual penetration testing by certified security auditors.

5.4 Data breach response

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the relevant supervisory authority within 72 hours of becoming aware of the breach. If the breach is likely to result in high risk to your rights and freedoms, we will also notify affected individuals without undue delay.

6.0 Data retention

6.1 How long will you use my personal data for?

Your information is securely stored. Neuro Notion App Limited will retain your personal data only for as long as is necessary for the purposes set out in this Privacy Notice. We will retain and use your personal data to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our legal agreements and policies.

To determine the appropriate retention period for personal data, 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 it, and applicable legal, regulatory, tax, accounting or other requirements.

- Your account content (conversations, tasks, routines, journal and mood entries, questionnaire answers): retained while your account is open.
- Inactive accounts: accounts inactive for 24 months are closed and deleted.
- System logs: kept for 12 months, and never more than 24 months.
- Analytics data: aggregated and anonymised, and may be kept indefinitely.
- Backups: Supabase takes daily backups with point-in-time recovery, kept for 7 days. A weekly encrypted copy is kept outside Supabase for 90 days.
- Deleted accounts: when an account is deleted, its data is removed from live systems within 30 days and is gone from all backups within 90 days, aside from AI memory notes held by Mem0, which we delete manually. Any data under a legal hold is kept as required by law.
- Billing and payment records: 6 years, as required by law.
- Clinic patients' data where we act as the clinic's processor: kept and deleted as set out in the clinic's contract, and returned or deleted when the contract ends.

In some circumstances we will anonymise your personal data for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

7.0 Protecting your sensitive data

Neuro Notion App Limited **follows the information security values of:**

Confidentiality: making sure your information is always kept secret and private;

Integrity: ensuring the completeness, consistency and accuracy of the data over its lifecycle; and

Availability: ensuring the right information is available to the right person at the right time.

8.0 Your legal rights

You have a number of rights under data protection laws in relation to your personal data. You have the right to:

- **Request access to your personal data** (commonly known as a subject access request). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data in certain circumstances. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest as the legal basis, or at any time where we are processing your personal data for direct marketing purposes.
- **Request the transfer** of your personal data to you or to a third party in a structured, commonly used, machine-readable format.
- **Withdraw consent** at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.
- **Request restriction of processing** of your personal data in certain circumstances, including where you want us to establish the data's accuracy or where our use of the data is unlawful.

If you wish to exercise any of the rights set out above, please contact us at vlad@romiadhd.com. You will not have to pay a fee to access your personal data (or to exercise any of the other rights) unless your request is clearly unfounded, repetitive or excessive. We try to respond to all legitimate requests within one month.

If your account is linked to a Healthcare Provider under a DPA, they are the Controller of your health data. While you can request rights directly from us, we may need to forward your request to your Healthcare Provider for their authorisation before acting on it.

9.0 Children's privacy

Our service is not intended for, nor do we knowingly collect personal information from, individuals under the age of 18 years. If we become aware that we have collected personal information from a child under the applicable age without verified parental consent, we will take immediate steps to delete such information. If you are a parent or guardian and you are aware that your child has provided us with personal data, please contact us at vlad@romiadhd.com.

10.0 Third-party links

Our app and website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our app or website, we encourage you to read the Privacy Notice of every website you visit.

11.0 Payments

We provide paid products and services within the app. We use Stripe, Inc. for payment processing. We will not store or collect your payment card details. That information is provided directly to Stripe, whose use of your personal information is governed by their own Privacy Notice. Stripe is PCI DSS Level 1 certified.

12.0 National Data Opt-Out (UK)

At this time, we do not share any personal data for planning or research purposes for which the national data opt-out would apply. We review all confidential patient information we process on an annual basis to see if it is used for research and planning purposes. If it is, then individuals can decide to stop their information being shared for that purpose. You can find out more information at https://www.nhs.uk/your-nhs-data-matters/

Where Romi is acting as a data processor on behalf of a Healthcare Provider, it is the responsibility of the data controller (the Healthcare Provider) to process the national data opt-out. Please contact your Healthcare Provider directly for further information.

13.0 Contact details

If you have any questions about this Privacy Notice or about the use of your personal data, or you want to exercise your privacy rights, please contact our Data Protection Officer:

Vlad Claudiu Bacila, Data Protection Officer

Neuro Notion App Limited

124 City Road, London, England, EC1V 2NX

Email: vlad@romiadhd.com

14.0 Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance at vlad@romiadhd.com.

15.0 Changes to the Privacy Notice and your duty to inform us of changes

We keep our Privacy Notice under regular review. This version was last updated on 20 November 2026. Material changes will be communicated through email notification to registered users, prominent notice on our website and within our services, and in-app notifications.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example a new email address.

16.0 Governing law and jurisdiction

This Privacy Notice and any disputes arising from or relating to the processing of personal data shall be governed by and construed in accordance with the laws of England and Wales. Any legal proceedings arising from this Notice shall be subject to the exclusive jurisdiction of the courts of England and Wales.

For users located in the European Union, this Notice shall also comply with applicable EU data protection laws, and you retain all rights granted under the GDPR and local implementing legislation.