

Privacy Policy — Neurree

Last updated: January 25, 2026

1. Introduction

Welcome to **Neurree**. Your privacy matters to us. This Privacy Policy explains how the app publisher (the “Publisher”, “we”, “us”, or “our”) collects, uses, stores, shares, and protects personal data when you use our mobile (IOS and Android) application **Neurree** (the “App”) and the Web Page (Neurree.com), and how you can exercise your rights under applicable data protection laws.

This policy applies only to personal data collected through the Web Page and the App and the services it provides.

This document explains the type, purpose and scope of data collection in connection with the use of our products.

The following notes provide a simple overview of what happens to your personal data when you visit or use our App. Personal data are all data with which you can be personally identified. For detailed information on data protection, please refer to our privacy policy listed below this text.

We would like to point out that data transmission over the Internet may have security gaps. It is not possible to completely protect data from access by third parties.

2. Data controller

Data controller: Erik Shikhverdiev, Individual publisher of Neurree

Contact: support@neurree.com (please use subject: "Privacy Inquiry")

Address: 120 Bayview Ave, Toronto, ON M5A 0J1, Canada

Data protection contact

Email: support@neurree.com

2. Users rights

General

The GDPR grants data subjects whose personal data are processed by us certain rights about which we would like to inform you at this point:

Revocation of your consent to data processing

Many data processing operations are only possible with your consent. We will expressly obtain this from you before we start processing the data. You can revoke this consent at any time. For this purpose, an informal notification by email to us is sufficient. The legality of the

data processing operations carried out up to the point of revocation remains unaffected by the revocation.

Right to object to data collection in special cases and in case of direct advertising (Article 21 GDPR)

If the data processing is carried out on the basis of Article 6 (1) (E) or (F) GDPR, you have the right at any time to object, for reasons arising from your particular situation, to the processing of personal data concerning you, which also applies to profiling based on these provisions.

The respective legal basis on which processing is based can be found in this privacy policy.

If you object, we will no longer process the personal data concerned unless we can prove that there are valid reasons for processing worthy of protection which outweigh your interests, rights and freedoms or which serve the processing of the assertion, exercise or defence of legal claims.

If your personal data are processed for the purpose of direct marketing, you have the right to object, at any time, to the processing of your personal data for the purpose of such marketing, including profiling, insofar as it is connected with such direct marketing. If you object, your personal data will no longer be used for the purpose of direct marketing.

Right of appeal to a supervisory authority

In the event of violations of the GDPR, those affected have a right of appeal to a supervisory authority. This right of appeal is without prejudice to other administrative or judicial remedies.

Information, deletion and correction

You have the right to receive information free of charge at any time about your stored personal data, its origin and recipients and the purpose of data processing, as well as the right to correct or delete this data. You can contact us at any time by email for this purpose and for further questions on the subject of personal data.

Right to restricting of processing

You have the right to request that the processing of your personal data be restricted. For this purpose, you can contact us at any time by email. The right to limit processing exists in the following cases:

If you dispute the accuracy of your personal data stored with us, we usually need time to verify this. For the duration of the review, you have the right to demand the restriction of the processing of your personal data.

If the processing of your personal data was/is unlawful, you can demand the restriction of data processing instead of deletion.

If we no longer need your personal data, but you need it for the exercise, defence or assertion of legal claims, you have the right to demand the restriction of the processing of your personal data instead of deletion.

If you have lodged an objection in accordance with Article 21 (1) GDPR, a balance must be struck between your interests and ours. As long as it is not yet clear whose interests prevail, you have the right to demand the restriction of the processing of your personal data.

If you have restricted the processing of your personal data, this data - apart from its storage - may only be processed with your consent or for the assertion, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of an important public interest of the European Union or a member state.

Right to data portability

You have the right to have data, which we process automatically on the basis of your consent or in fulfillment of a contract, handed over to you or to a third party in a common, machine-readable format. If you request the direct transfer of the data to another responsible party, this will only be done to the extent technically feasible.

3. Summary — What we collect and why

General information on data retention for personal data

Subject to deviating or more specific information within this privacy policy, the personal data collected by this App will be stored until you request us to delete it, revoke your consent for storage or the purpose for which the data was stored ceases to apply. If there is a legal obligation to store the data or any other legally recognized reason for storing the data (e.g. legitimate interest), the personal data concerned will not be deleted until the respective reason for storage no longer applies.

Legal basis for the storage of personal data

The processing of personal data is only permitted if there is an effective legal basis for the processing of such data. If we process your data, this is regularly done on the basis of your consent in accordance with Article 6 (1) (a) General Data Protection Regulation (GDPR) (e.g. when you voluntarily provide your data in the registration form or in the contact form), for the purpose of fulfilling the contract in accordance with Article 6 (1) (b) GDPR (e.g. when using In-APP purchases or the use of other chargeable functions of the PRODUCT) or on the basis of legitimate interests according to Article 6 (1) (f) GDPR, which are always weighed against your interests (e.g. in the context of advertising measures). The relevant legal basis will be specified in a separate place in this privacy policy.

Encryption

This PRODUCT uses SSL or TLS encryption for reasons of security and to protect the transmission of confidential content, such as the requests you send to us as the operator, or communication between users or payment data (e.g. account number for direct debit authorization, Visa/MasterCard, direct debit). This encryption prevents the data you transmit from being read by unauthorized third parties.

On the WEB: You can recognize an encrypted connection by the fact that the address line of your browser changes from "http://" to "https://" and by the lock symbol in your browser line.

Changes to this privacy policy

We reserve the right to change these data protection regulations at any time in compliance with legal requirements.

Access rights of the APP

In order to provide our services via the APP, we require the access rights listed below, which enable us to access certain functions of your device.

- Wi-Fi connections
- Receiving data from the Internet
- Network access
- Power saving mode (prevent the "sleep mode" from being activated on the device)
- Vibration control

Access to the device functions is required to ensure the functionality of the APP. The legal basis for this data processing is our legitimate interest within the meaning of Article 6 (1) (f) GDPR, your consent within the meaning of Article 6 (1) (a) GDPR and/or - if a contract has been concluded - the fulfillment of our contractual obligations (Article 6 (1) (b) GDPR).

The data collected in this way will be stored until the User submits a request for its deletion, as provided in 12.3 of the Policy.

Minimum data we collect to operate the App:

- **Email address** — required to create and manage your account, send important service messages, and authenticate you.
- **Username / login** — chosen by you for identification in the App.
- **Password** — used for authentication. We do **not** store passwords in plain text; we use industry standard safeguards (see Security below).

Purpose of processing: to provide the App's features, secure and maintain your account, communicate about your account and updates, and comply with legal obligations.

If you do not provide the required account information we cannot create an account or provide the core service.

4. Collection of personal data in the context of the use of the App

4.1 Account information (required)

- **Email address, username, password.**

General

When you use our PRODUCT, we collect the following personal data from you, depending on availability:

- Usage data
- Metadata
- IP address
- Device identification
- Email address
- ID of social networks / external service providers when registering externally (if activated, see below for the individual service providers such as Facebook Connect, Google Account, Apple login)

The processing of this personal data is necessary to guarantee the functionalities of the PRODUCT. The legal basis for this data processing is our legitimate interest within the meaning of Article 6 (1) (f) GDPR, your consent within the meaning of Article 6 (1) (a) GDPR and/or - if a contract has been concluded - the fulfillment of our contractual obligations (Article 6 (1) (b) GDPR).

4.2 Optional / additional data

- We will only collect additional personal data if you voluntarily provide it (for example, if you choose to supply a profile name or contact details). Any optional data collection will be explained at the time of collection.

We do **not** collect or process special category (sensitive) data such as health information, racial or ethnic origin, political opinions, religious beliefs, or biometric data.

4.3 Server log files

The provider of the pages automatically collects and stores information in so-called server log files, which your browser or the PRODUCT automatically sends to us. These are:

- Operating system used
- Hostname of the accessing computer
- Time of the server request
- IP address
- WEB: Browser type and version
- WEB: Referrer URL

This data is not merged with other data sources.

The collection of these data is based on Article 6 (1) (f) GDPR. The operator has a legitimate interest in the technically error-free display and optimization of his application - for this purpose the server log files must be recorded.

4.4 Registration in the PRODUCT

You need to register in the PRODUCT to use its core features. We will use the data entered for this purpose only for the purpose of using the respective offer or service for which you

have registered. The mandatory data requested during registration must be provided in full. Otherwise, we will refuse the registration.

In the event of important changes, for example in the scope of the offer or technically necessary changes, we will use the email address provided during registration to inform you in this way.

The data entered during registration is processed for the purpose of implementing the user relationship established by the registration and, if applicable, for the initiation of further contracts (Article 6 (1) (b) GDPR).

Retention of the data entered during registration is stored in line with Section 10 of the Policy. Legal retention periods remain unaffected.

4.5 Registration with Google Account

Instead of a direct registration you can register with your Google Account.

The provider of this service is Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland. However, according to Google, the data collected is also transferred to the USA and other third countries.

If you choose to register with your Google Account and click on the button, you will be automatically redirected to the Google platform. There you can log in with your usage data. This will link your Google Account with this PRODUCT or our services. This link gives us access to your data stored at Google. This is above all:

Email address

This data is used to set up, provision and personalize your account.

The registration with your Google Account and the associated data processing procedures are based on your consent (Article 6 (1) (a) GDPR). You can revoke this consent at any time with effect for the future.

You can find further information in the Google Terms of Use and the Google Privacy Policy. These can be found under:

<https://policies.google.com/privacy?hl=de> and <https://policies.google.com/terms?hl=de>

4.6 Request within the PRODUCT, by email or by phone

If you contact us (e.g. via contact form within the PRODUCT, by email, telephone or fax), your inquiry including all personal data resulting from it (e.g. name, inquiry) will be stored and processed by us for the purpose of processing your request. This data is processed on the basis of Article 6 (1) (b) GDPR, provided that your inquiry is related to the fulfilment of a contract or is necessary for the implementation of pre-contractual measures. In all other cases the processing is based on your consent (Article 6 (1) (a) GDPR) and/or on our legitimate interests (Article 6 (1) (f) GDPR), as we have a legitimate interest in the effective processing of the inquiries addressed to us. The data sent to us by you via contact request will remain

with us until you request us to delete it, revoke your consent for storage or the purpose for which the data was stored no longer applies (e.g. after your request has been processed). Mandatory legal provisions - in particular legal retention periods - remain unaffected. We will not pass on your data without your consent.

4.7 Newsletter data

If you would like to receive the newsletter offered in our PRODUCT, we need an email address from you as well as information that allows us to verify that you are the owner of the email address provided and that you agree to receive the newsletter. Further data will not be collected. We use these data exclusively for sending the requested information and do not pass them on to third parties. The dispatch of the newsletter is based on your consent (Article 6 (1) (a) GDPR). You can revoke this consent at any time.

For the maintenance and analysis of our newsletters we use the following data through our service providers:

- Opening of emails
- Clicks on emails
- Newsletter subscriptions

4.8 Google Firebase

This service is provided by Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. The use of Google Firebase may require the transfer of your personal data to the USA.

Firebase is part of the Google Cloud Platform (Google Ireland Limited, Gordon House, Barrow Street, Sieblin 4, Ireland) and offers various services for web and app developers (<https://firebase.google.com/terms/>). Some Firebase services process personal data. In most cases, the personal data used is limited to so-called instance IDs, which are time-stamped. The instance IDs created by Firebase are only used once and therefore allow the assignment to certain events or processes. According to Google, the data collected in this process is not personal data.

In other cases, Google Firebase stores, among other things, the number and duration of sessions, operating systems, device models, region and a number of other data. A detailed overview of the data collected by Google Firebase can be found at: <https://support.google.com/firebase/answer/6318039>

For Analytics for Firebase Google uses not only the above mentioned instance ID, but also the advertising ID of the end device. You can change the usage of the Ad ID in the device settings of your mobile device.

Android: Settings > Google > Ads > Reset Ad ID

iOS: Settings > Privacy > Advertising > No Ad Tracking

We use Google Firebase above all:

to select configuration data necessary for operation and to transfer this data to end user devices

to analyze user behavior and solve problems in the user experience, for example by evaluating crash reports

to open newly installed apps on a specific page or in a specific context

to send push notifications or so-called in-app messages (notifications that are only displayed in the respective PRODUCT). You can disable and enable push notifications at any time through your device settings.

The paragraph at the top ("General information on data retention for personal data") applies to the storage period of data collected in this way. Personal data at Google Firebase is not stored longer than necessary for the purpose of the service (usually up to 14 months). Further information can be found under:

<https://support.google.com/analytics/answer/7667196?hl=de-DE>

Google Firebase is used to optimize this PRODUCT and to improve our offers. This represents a legitimate interest in the sense of Article 6 (1) (f) GDPR.

Further information about Google Firebase can be found at:

<https://firebase.google.com/>

<https://www.firebase.com/terms/privacy-policy.html>

4.9 Data Analysis

If you access our PRODUCT, your behavior can be statistically evaluated with the help of certain analysis tools and analyzed for advertising and market research purposes or to improve our offers. When using such tools, we ensure that the legal data protection regulations are observed. When using external service providers (contract processors), we ensure through appropriate contracts with the service providers that the data processing complies with European data protection standards.

5. Legal bases for processing (GDPR)

Where the GDPR applies, we rely on the following legal bases to process your personal data:

- **Performance of a contract:** to create and operate your account, authenticate you, and provide the App's functionality.
- **Legitimate interests:** to secure the App and users (fraud prevention and security), to operate, improve and analyze our services, and to enforce our terms and policies, provided these interests do not override your rights and freedoms.
- **Consent:** where required (for instance, to send marketing communications). You can withdraw consent at any time.
- **Legal obligations:** to comply with laws, court orders, or requests from public authorities.

Under Canadian law, we process personal data with your knowledge and consent, except where otherwise permitted or required by law.

6. How we use your information

We use personal data for the following purposes:

- **Account creation and authentication.**
- **Service delivery and maintenance** of your account and core App features.
- **Security and fraud prevention**, including detecting and responding to suspicious activity.
- **Communications**: sending transactional messages such as account confirmations, password resets, security alerts, and important service notices.
- **Marketing and promotions** only if you opt in. You may unsubscribe at any time.
- **Legal compliance** (e.g., responding to lawful requests from authorities).

7. Third-party processors and data hosting

To provide the App we use third-party processors that host, maintain, or help operate our service. These processors act on our instructions and are bound by contract to protect your personal data.

Key processors:

- **Database provider**: Neon (Neon SaaS Postgres) — used to store account data.
- **Server hosting / infrastructure**: Heroku (hosted in the European Union region).

Notes on processors and transfers:

- Your account data is stored in the infrastructure noted above. Where any personal data is transferred outside the European Economic Area (EEA), we will rely on an adequacy decision or implement appropriate safeguards to ensure an adequate level of protection.
- We may engage additional subprocessors (payment processors, analytics, customer support tools) **in the future**; we will require appropriate contractual protections.

8. Data sharing and disclosure

We will not sell your personal data. We may disclose personal data to:

- **Service providers and subprocessors** for the purposes described in this policy.
- **Business transfers** only in connection with a merger, sale, or reorganization; in such cases we will use reasonable efforts to require the transferee to honor this Privacy Policy.
- **Law enforcement or regulators** when required by applicable law.

9. International transfers

While our main infrastructure for the App is hosted within the European Union, some subprocessors or backup locations may be outside the EEA or Canada. When personal data is transferred internationally, we will protect it using legal mechanisms such as:

- An adequacy decision by the European Commission; or
- Standard Contractual Clauses; or
- Other GDPR/Canadian privacy law-compliant safeguards.

10. Data retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including to:

- Provide and operate the App while your account is active.
- Comply with legal obligations and resolve disputes.

If you request account deletion, we will delete or anonymize your personal data as required by applicable law, subject to any legal exceptions.

11. Security measures

We implement industry-standard technical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, including:

- Transport-layer encryption (TLS) for data in transit.
- Encryption and access controls where supported by our hosting and database providers.
- Storing passwords using secure hashing (and salting) techniques — we do not store passwords as plain text.
- Limiting internal access to personal data on a need-to-know basis.
- Periodic security reviews and patching of systems.

Important: no system can be 100% secure. If we become aware 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 and affected data subjects in accordance with GDPR timelines (generally within 72 hours to the authority, and without undue delay to affected individuals when required).

12. Your rights under GDPR and Canadian law

12.1. If you are located in the EU/EEA, you have the following rights regarding your personal data (subject to legal limits):

- **Right of access** — request a copy of the personal data we hold about you.
- **Right to rectification** — correct inaccurate or incomplete data.
- **Right to erasure** ("right to be forgotten") — request deletion of personal data in certain situations.

- **Right to restrict processing** — ask us to limit how we process your data.
- **Right to data portability** — receive your data in a machine-readable format and transfer it to another controller where applicable.
- **Right to object** — object to processing based on legitimate interests or direct marketing.
- **Right to withdraw consent** — where processing is based on consent, you may withdraw it at any time (this does not affect processing prior to withdrawal).

12.2. Under Canadian privacy law, you also have the right to:

- **Access** the personal information we hold about you.
- **Request correction** of inaccurate or incomplete information.
- **Withdraw consent** to the collection, use, or disclosure of your information, subject to legal and contractual restrictions.

12.3. How to exercise your rights: Contact us at **support@neurree.com** with the subject line "**Data Subject Request**" and indicate the request type (e.g., access, deletion). We will verify your identity before fulfilling a request and respond within one month in accordance with GDPR or within a reasonable time under Canadian law.

12.4. If you believe we have violated your rights, you may lodge a complaint with your local data protection authority (for example, the supervisory authority in the EU member state where you live, or the Office of the Privacy Commissioner of Canada).

13. Children's privacy

The App is **not** intended for children under the age of **18**. We do not knowingly collect personal data from children under this age. If you are a parent or guardian and believe we have collected personal data about a child under 18, please contact us at **support@neurree.com** and we will delete the information where required by law.

14. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes to our practices, services, legal requirements, or for operational reasons. We will publish the revised policy in the App and update the "Last updated" date. Where required by law, we will notify you in advance and request the consent of material changes.

15. How to contact us

For privacy-related questions, data subject requests, or complaints, please email: **support@neurree.com**

If you prefer, you can write to us at:

120 Bayview Ave, Toronto, ON M5A 0J1, Canada