

Privacy Policy

Introduction

We, at DNA ERA s. r. o. (referred to in this policy as "we", "us" or "DNA ERA", "the Company") truly value your privacy. We are committed to the protection of your personal data, and do not access or use it for any purpose other than providing, maintaining and improving the **Talk to Your Genes** mobile application ("the App") and its related services, and as otherwise required by law.

This policy outlines how we manage such information to ensure we meet our obligations to respect your privacy and that all such information remains confidential. The policy explains our binding obligations which come from the terms of:

- the General Data Protection Regulation (GDPR) (EU) 2016/679;
- Act No. 18/2018 Coll. on the Protection of Personal Data (Slovak Republic), adopted for the effective implementation of the GDPR; and
- any applicable data protection law as amended from time to time.

Who are we?

DNA ERA s. r. o. is the **data controller**. This means we are responsible for determining the purpose and manner in which your personal data is used.

We are committed to doing the right thing when it comes to how we collect, use and protect your personal data and that is why we have developed this Privacy Policy, which:

- Sets out the different ways you interact with us and the types of personal data that we collect;
- Explains the reasons why we use the data we collect;
- Explains when and why we will share personal data with other organisations; and
- Explains the rights and choices you have when it comes to your personal data.

Our details

DNA ERA s. r. o. is a limited liability company incorporated under the laws of the Slovak Republic.

DNA ERA s. r. o.

Email: info@dnaera.com

Address: Karadžičova 8, 821 08 Bratislava - Ružinov, Slovak Republic

What do we mean by personal data?

Personal data is any information relating to you or data that may be used to identify you.

As a user of our App, you provide us with some of your personal data, which will include your name and email address used to register your account. It may also include IP addresses, device and browser information, and other account usage information, which in some circumstances may be used to identify you.

Genetic data derived from your DNA test kit is processed by us as part of the core service. Genetic data is classified as a **special category of personal data** under Article 9 of the GDPR and is subject to stricter protections. We process such data only with your explicit consent and only to the extent necessary to provide you with personalised genetic insights.

What sort of information do we need and why?

When you access the App, we may collect personal data when you log in with your existing account credentials, submit your DNA sample, contact us, or otherwise use our services.

We process the personal data we receive from you as part of our service relationship with you when you access Talk to Your Genes. We do this under the legal grounds of 'performance of a contract' and, where applicable, 'explicit consent' for special category data. The types of personal data we need and the reasons we need it are detailed below:

What do we collect?	Why?
Your name, email address, and login credentials.	To authenticate and manage your account and identify you as a user.
DNA test results and genetic data derived from your submitted DNA sample.	To generate your personalised genetic insights, reports, and recommendations within the App. This is the core purpose of the service.

What do we collect?	Why?
Device information such as device model, operating system version, app version, IP address, and crash logs.	To maintain app stability, diagnose technical issues, and improve the user experience.
Support communications — emails, in-app messages, or other correspondence you send us.	To respond to your requests and resolve issues.
Any other personal information.	In order to comply with applicable rules, laws and regulations.

How is your personal data collected?

We collect most of this personal data directly from you, via the App or by email. However, in some instances:

- a. We will request information from you through the App's login flow and account settings, and use our own records and information from partner laboratories for the purpose of delivering your genetic results and complying with applicable obligations.
- b. The processing and storage of your personal data are necessary to provide you with the Talk to Your Genes service. If you choose not to provide the requested information, we may not be able to authenticate you or deliver the full service.

We keep the information as up-to-date as possible and will update any details promptly when you notify us of a change.

Your use of the App involves the automated collection of certain types of information, some of which may be considered personal data. This includes: IP address, device type, operating system, and app usage data.

Why do we need this information and on what legal basis is the data processed?

Lawfulness of processing

We will process your personal data (to collect, use, store and transfer, where necessary) in order to:

- a. perform the service agreement between you and us and provide you with Talk to Your Genes;
- b. process your DNA sample and generate personalised genetic insights;
- c. comply with any and all applicable legal and regulatory obligations, including Slovak data protection law and the GDPR;
- d. pursue our legitimate interests — for example, to ensure the App functions correctly, to prevent fraud, and to improve our services in your best interest; and
- e. if you have given us consent — for example, for marketing or promotional communications. Any consent given may be revoked at any time by you with future effect.

Purposes

We will process your personal data in combination with your use of the App for the purposes of:

- a. providing the Talk to Your Genes service to you;
- b. verifying your identity and managing your account;
- c. processing your DNA test results and generating reports and insights;
- d. communicating with you regarding your account or the service by email or in-app notification;
- e. responding to your support requests;
- f. conducting risk management, data analysis, and monitoring to ensure the ongoing quality of the service;
- g. enhancing, improving and personalising the App to better your experience;
- h. sending you important account and service-related information;
- i. preventing misuse and fraud and maintaining the security of the App;
- j. managing disputes, complaints, or legal proceedings; and
- k. marketing communications about updates to our products and services, where you have consented or where it is in our legitimate interest, and you have not opted out.

Who receives your personal data?

Your personal data is received and processed by employees of DNA ERA s. r. o. for the execution of contractual and legal obligations. We will never sell your personal data to third parties. We may disclose your data where necessary to satisfy the purposes set out above, to the following recipients:

- a. **Partner laboratories** — accredited laboratories that process your DNA sample on our behalf. They are only authorised to process your data strictly for the purposes of analysing your sample and returning results to us.
- b. **Technology and infrastructure providers** — third-party services that provide cloud hosting, analytics, and other IT infrastructure to the Company. These providers are only authorised to process your data in accordance with our instructions and are bound by appropriate data processing agreements.
- c. **Professional advisors** — lawyers, external auditors, or other advisors, as well as courts, regulatory, governmental, or other official bodies, where disclosure is necessary (i) to comply with any applicable law or regulation; (ii) to enforce applicable terms and conditions; (iii) to protect the security or integrity of our services; or (iv) to protect our rights and interests.
- d. **Third parties in the context of mergers and acquisitions** — provided that the prospective buyer or successor agrees to respect your personal data in a manner consistent with this Privacy Policy.

We will require any entity to whom we disclose your information to ensure its confidentiality and to handle it in line with the legitimate purpose for which they are allowed to access it, and in accordance with applicable data protection laws.

We will not sell your personal data with third parties for their own independent marketing or business purposes without your consent.

AI and Automated Decision-Making

The App uses artificial intelligence ("AI") to deliver its core features. These features involve automated processing of information derived from your genetic profile, specifically to:

- a. Select which aspects of your genetic profile to highlight for you on a given day, based on factors such as significance, recency of previous recommendations, and relevance to your overall genetic profile;
- b. Generate natural-language stories and recommendations tailored to your genetic profile;
- c. Compose push notifications that encourage engagement with your genetic insights; and
- d. Provide conversational responses in the in-app chat that reference your genetic profile.

To deliver these features, we send the following data to **Google LLC**, through its Gemini API: (i) a summary of your genetic results derived from your DNA ERA analysis; (ii) profile details you have provided — sex, age, height and weight; and (iii) the content of your messages in the in-app chat, including the conversation history of the chat you are in. No other data is

sent — we do not send your name, e-mail address, account identifier, or your raw genetic sequencing data.

Google acts solely as our data processor under a written data processing agreement, and processes this data only to generate the response returned to you. Google does not use it to train its models and does not use it for any other purpose. Google is contractually bound to provide the same or equal protection of your personal data as set out in this Privacy Policy. Data may be processed outside the EU/EEA under the safeguards described in "Transferring information internationally".

We ask for your explicit consent inside the App before any of this data is sent. The consent screen appears at the end of the introductory questionnaire, before the chat is available, and names Google and each category of data listed above. Consent is required to use the App: the chat is its core feature, so if you do not consent you do not reach it and no data is sent to Google.

You can withdraw your consent at any time in Settings → Withdraw AI consent. Because the App cannot provide its service without this processing, withdrawing your consent means deleting your account: the option starts an account deletion request, we confirm it by e-mail, and from then on no data of yours is sent to Google. You may also exercise the erasure right described in "What are your rights?" below, or contact us at info@dnaera.com.

Nature of decisions

The AI-generated content in the App is informational and educational in nature. It does not constitute medical advice, a medical diagnosis, or a treatment recommendation. No decisions with legal or similarly significant effects are made about you solely on the basis of automated processing.

Your rights regarding automated processing

Under Article 22 of the GDPR, you have the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significantly affects you. While we do not believe the App's AI features fall within the scope of Article 22, we nevertheless provide you with the ability to:

- a. Request meaningful information about the logic involved in the automated processing;
- b. Express your point of view and contest any output you believe to be inaccurate or inappropriate; and
- c. Request human review of any AI-generated content by contacting us at info@dnaera.com.

Push Notifications

With your permission, the App may send you push notifications containing personalised content generated using the automated processing described above. You may disable push notifications at any time through your device settings (iOS: Settings > Notifications > Talk to Your Genes; Android: Settings > Apps > Talk to Your Genes > Notifications). Disabling notifications will not affect your ability to access insights within the App.

Chat and Conversation Data

When you use the in-app chat, we collect and store the messages you send, the responses generated by the AI, and the date and time of each interaction. Chat data is retained for the duration of your active account and is deleted in accordance with the retention periods described in the 'How long will your data be stored?' section. Chat data is not used to train AI models and is not shared with third parties beyond what is necessary to generate your responses.

Age Restriction and Children's Data

The App is intended for users aged **18 years and older**. Users under the age of 18 may only use the App and its services with the consent and involvement of a legal guardian. We do not knowingly collect personal data from individuals under the age of 18 without such consent.

If we become aware that we have collected personal data from a person under 18 without appropriate legal guardian consent, we will take steps to delete that information as soon as possible. If you believe we may have collected such data, please contact us at info@dnaera.com.

Your Genetic Data — Additional Provisions

Given the sensitive nature of genetic information, we apply the following additional safeguards:

- a. **Storage:** We store derived genetic traits and interpreted results necessary to operate the App. Raw sequencing data, once processed by our partner laboratory, is not retained by us in its raw form unless required to deliver the service.
- b. **No insurance or employer sharing:** Your genetic data will never be shared with insurance companies, employers, or any third party for underwriting, employment, or eligibility decisions.

- c. **No research use without consent:** Your genetic data will not be used for scientific research or statistical purposes unless you provide separate, specific consent for such use.
- d. **Physical sample:** Your physical DNA sample is destroyed after genotyping. Only the raw data prepared for analysis is retained.

Analytics and Tracking Technologies

The App may use third-party analytics tools to help us understand how the App is used, diagnose technical issues, and improve the user experience. These tools may collect information such as device type, operating system, app version, session duration, and feature usage patterns.

Analytics data is collected in aggregated or pseudonymised form wherever possible. Your health and genetic data is never shared with analytics providers.

Transferring information internationally

Personal data may be held at our offices and with our third-party service providers as described above. Some of these third parties may be based outside the EU and the European Economic Area (EEA).

Under data protection law, we may only transfer your personal data to a country or international organisation outside the EU/EEA where:

- a. the European Commission has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'adequacy decision');
- b. there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- c. a specific exception applies under data protection law.

Adequacy decision

We may transfer your personal data to certain countries on the basis of an adequacy decision between the EU/EEA and other jurisdictions. We will always seek to rely on an adequacy decision where one exists.

Transfers with appropriate safeguards

Where there is no adequacy decision, we may transfer your personal data only if we are satisfied that the transfer complies with data protection law, that appropriate safeguards are

in place (such as Standard Contractual Clauses approved by the European Commission), and that enforceable rights and effective legal remedies are available to you.

How long will your data be stored?

We will process your personal data for the duration of your active account with us and for a period of **3 (three) years** after account deletion or the termination of our service relationship, unless a longer retention period is required by applicable law.

Any personal data will not be retained for longer than the time necessary in order to satisfy the purposes of its processing, subject to applicable statutory limitation periods. Once data is no longer needed, it is securely deleted or anonymised.

What are your rights?

You have a number of rights when it comes to how we handle your data. Some of these are the:

a. Right of access:

You can access and obtain information about your personal data — you have the right to request what information (if any) we process for you and, if so, receive a copy of that personal data. To make a request, contact us using the details in the 'How to contact us' section below. We will need to verify your identity before responding. We will acknowledge your request and respond within one month of receipt.

b. Right to rectify:

You can rectify any factual inaccuracies or incompleteness with respect to your personal data. If the data we hold about you is inaccurate or incomplete, you may ask us to correct it. We will acknowledge and respond within one month.

c. Right to erasure:

You can request deletion of your personal data — you can ask us to delete or remove your personal data in cases where we no longer need it. You may also delete your account directly from within the App. Please note that such a request will be satisfied provided that we have no legal obligation to retain such data, subject to any applicable retention periods.

d. Right to restrict processing:

You can ask us to restrict the processing of your personal data in certain circumstances, such as when you contest the accuracy of the information or believe the processing is unlawful.

e. **Right to object:**

You can object to the processing of your personal data where we are relying on our own legitimate interests or where the data is being processed for direct marketing purposes.

f. **Right to data portability:**

You have the right, where applicable, to receive the personal data you have provided to us in a structured, commonly used and machine-readable format, and to transmit that data to another controller of your choice where technically possible.

g. **Right to withdraw consent:**

Where processing is based on your consent (for example, marketing communications), you may withdraw consent at any time with future effect, without affecting the lawfulness of processing carried out before withdrawal.

h. **Right to complain:**

You have the right to lodge a complaint with the Slovak supervisory authority regarding our processing of your personal data (see 'How to contact us' section below for details).

Please contact us using the details provided in the 'How to contact us' section to make a request. We will do our best to respond within 30 days of receiving such a request. If we cannot respond within that period, we will let you know the reasons why and when we expect to be able to fulfil your request.

How do we safeguard your personal data?

We put significant effort into ensuring that your personal data is secured and kept confidential. Any personal data you provide to us is stored on secure servers, and we use rigorous procedures to protect against loss, misuse, unauthorised access, alteration, disclosure, or destruction of your personal data. The measures we apply include, among others:

- a. **Encryption** — personal data is encrypted in transit (TLS/HTTPS) and at rest, making it unreadable to unauthorised users;
- b. **Minimisation** — the personal data we collect is adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- c. **Access controls** — access to your personal data is permitted only to employees who need it to properly exercise their professional duties;
- d. **Security testing** — we perform regular assessments to identify potential security vulnerabilities and apply remedies to address them; and
- e. **Training** — we ensure our team has the appropriate knowledge to manage your data securely and in compliance with applicable law.

We maintain security and incident response plans to handle any physical or technical incident in a timely manner and to limit any negative effect. Although we work hard to protect your personal data, we cannot guarantee that our safeguards will prevent every unauthorised attempt to access, use or disclose it.

Your role

Please recognise that you play a vital role in protecting your own personal data. When using the App, it is important to choose a strong password, not share it with any third parties, and immediately notify us if you become aware of any unauthorised access to or use of your account. It is your responsibility to ensure your login credentials are kept safe.

How will we store your personal data?

Your information will be held on our secure servers and, where applicable, on the secure systems of our third-party infrastructure providers. We have in place systems and procedures to prevent unauthorised access, improper modification or disclosure, misuse or loss of information.

We will hold your information for the retention periods described in the 'How long will your data be stored?' section above. Once we determine that such information is no longer needed, we will securely delete or destroy it.

Data Protection Officer

Given the nature of the data we process, including special categories of personal data, we have designated a point of contact for all data protection matters. For any questions or concerns regarding how your personal data is processed, you may reach our data protection contact at:

Email: info@dnaera.com

How to contact us and how to complain?

If you have any questions with regard to your rights or this policy, or if you consider that we have failed to respect your privacy, you may contact us by:

Email: info@dnaera.com

Address: Karadžičova 8, 821 08 Bratislava - Ružinov, Slovak Republic

If you are not satisfied with our response to your complaint in respect of your personal data, you have the right to lodge a complaint with the Slovak supervisory authority for personal data protection:

Úrad na ochranu osobných údajov Slovenskej republiky

(Office for Personal Data Protection of the Slovak Republic)

Hraničná 12, 820 07 Bratislava 27, Slovak Republic

Web: www.dataprotection.gov.sk

Tel: +421 2 3231 3214

Linking to Other Websites

If you access any links to third-party websites from within the App or our communications, please be aware that those websites have their own privacy policies. We do not accept any responsibility or liability for those policies. You should review them before submitting any personal data to those websites.

Changes to This Privacy Policy

We may change this Privacy Policy from time to time by posting the updated version on our website or within the App. Laws, regulations and industry standards evolve, which may make those changes necessary, or we may make changes to our business. We advise you to review this policy regularly to stay informed and to make sure that you are happy with any changes. If you disagree with the changes to this Privacy Policy, you should discontinue your use of the App.

Personal Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Company is obliged to do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Company is required to also inform those individuals without undue delay.

A personal data breach is defined as having the potential to affect the confidentiality, integrity or availability of personal data held by the Company in any format. Such breaches may occur for a number of reasons, including:

- a. Disclosure of personal data to unauthorised persons;

- b. Loss or theft of data and/or equipment on which data is stored;
- c. Inappropriate access controls allowing unauthorised use of information;
- d. Breaches in the Company's IT systems and security;
- e. Unauthorised access to computer systems, e.g. hacking;
- f. Viruses or other security attacks; or
- g. Emails containing personal data sent in error to the wrong recipient.

Legal Disclaimer

The Company may disclose your personally identifiable information as required by rules and regulations, and when the Company believes that disclosure is necessary to protect our rights and/or to comply with any proceedings, court order, legal process served, or pursuant to governmental, intergovernmental or other regulatory bodies.

The Company shall not be liable for misuse or loss of personal information on any third-party website or platform that the Company does not have access to or control over. The Company will not be liable for unlawful or unauthorised use of your personal information due to misuse or misplacement of your passwords, negligent or malicious intervention, or otherwise due to your own acts or omissions.

Effective Date

This Privacy Policy is effective as of **3 September 2026** (version 1.0). Previous versions, if any, are available upon request.