LEAPR App Privacy Policy

("the Policy")

LEAPR is a gamified self-development app that offers voluntary daily challenges designed to build confidence in social situations. We take your privacy seriously.

LEAPR is a self-development and educational tool and does not constitute a medical or therapeutic service. Any wellbeing-related and psychological assessment data you provide is used solely for the purpose of personalising your experience within the App and is not used for any clinical, diagnostic, or research purposes. Further information regarding what LEAPR is and is not can be found in LEAPR Terms and Conditions.

The App may only be used by individuals who are at least 16 years of age. We do not knowingly collect personal data relating to individuals under the age of 16. If we become aware that such data has been collected, we will delete it without undue delay. Parents or legal guardians who believe that their child has created an account in the App should contact us at **privacy@leapr.app***, and we will take immediate action.*

By using the App, you acknowledge that you have read and understood this Privacy Policy.

Last updated: 27 August 2026

I. Who processes LEAPR Users' personal data?

1. The controller of the personal data of LEAPR App users (**"Users"**) is Dawid Ratajczak (**"LEAPR"**), address: Os. Stare Zegrze, 61-249 Poznań, Poland. Any matters relating to the processing of personal data may be directed to LEAPR at the following dedicated e-mail address: **privacy@leapr.app**.
2. LEAPR makes every effort to protect Users' personal data against unauthorised disclosure, unauthorised access, unlawful processing, alteration, loss, damage, or destruction and respects the privacy of every individual whose personal data it processes.
3. Personal data is processed by LEAPR in accordance with applicable law, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**"GDPR"**).
4. Capitalised terms used in this Policy shall have the meaning assigned to them in the LEAPR Terms and Conditions.
5. This Policy sets out the rules governing the processing and protection of Users' personal data, including:
    1) the categories of personal data collected by LEAPR in connection with the provision and administration of the App;
    2) the manner in which such data is used;
    3) Users' rights relating to the processing of their personal data;
    4) categories of recipients to whom personal data may be disclosed;
    5) measures implemented to safeguard and secure personal data; and
    6) methods of contact regarding the exercise of data subject rights.
6. The App is distributed through Apple App Store and Google Play. Use of these platforms may involve the processing of personal data in accordance with privacy policies of those entities, for which LEAPR accepts no responsibility.

II. How is Users' personal data collected?

1. LEAPR primarily obtains personal data directly from Users. In certain cases, depending on the nature of the data and the operation of the App, personal data may also be collected automatically through the App or obtained from third parties in accordance with this Policy.

2. Personal data is shared by the Users voluntary. However:

    1) personal data required for the creation and maintenance of the Account and for the supply of App services (marked as mandatory in relevant forms) is necessary for entering into and performing the agreement for the supply of electronic services and for accessing the App's core functionalities;

    2) data relating to activity and participation in Challenges is entirely voluntary and failure to provide such information will only result in reduced personalisation of Challenges and the overall App experience;

    3) marketing consents (e-mail communications and push notifications) are entirely voluntary and have no impact on the ability to use the App's basic functionalities; and

    4) other optional data (e.g. surveys, quizzes, voluntary submissions) may only affect the specific feature to which such data relates.

3. LEAPR may collect the following categories of personal data:

    1) contact details (e.g. e-mail address, username and password, or authentication tokens where the User signs in via Google Play or Apple App Store);

    2) information provided through questionnaires and surveys completed by the User (including psychological assessment questionnaires and "Post-Challenge Reflection" surveys);

    3) correspondence with the LEAPR Team

        - data collected directly from Users;

    4) information relating to the use of the App (e.g. initiated and completed Challenges, experience points (XP), achieved levels, streaks, App activity events and the use of App functionalities);

    5) technical information (e.g. device type and model, operating system and version, application version, language settings, time zone and approximate location inferred from device or network settings);

    6) diagnostic information (e.g. crash reports and performance logs used to identify and resolve technical issues);

    7) push notification tokens (e.g. device identifiers used for sending push notifications via Apple Push Notification Service [APNs] or Firebase Cloud Messaging [FCM])

        - data collected automatically;

    8) subscription and payment information; following the purchase of a subscription, LEAPR's payment service providers (including Apple App Store, Google Play and RevenueCat) provide confirmation of purchase, subscription status and limited transaction metadata

        - data obtained from third parties.

As part of Users' responses to psychological assessment questionnaires and other surveys or quizzes completed within the App, LEAPR may process special categories of personal data, including data concerning an individual's health and mental wellbeing within the meaning of Article 9(1) GDPR. Such data is processed solely on the basis of the User's explicit consent, which is requested separately and prominently before the User accesses the relevant questionnaire. Consent may be withdrawn at any time by contacting **privacy@leapr.app** or using the

relevant Account settings within the App. Withdrawal of consent may limit functionalities of the App that rely on such data.

Special categories of personal data are subject to enhanced protection measures. Such data:

1) is never disclosed to other Users;
2) is never sold or shared for advertising purposes;
3) is used exclusively to personalise the User's experience with Challenges; and
4) is subject to additional access restrictions within LEAPR's systems.

III. How is Users' personal data processed?

1. LEAPR ensures:
    1) control over the type and scope of Users' personal data being processed, the duration and method of such processing, as well as the persons authorised to process it;
    2) adequate administrative, technical and physical protection of Users' personal data against accidental, unlawful or unauthorised damage, loss, alteration, access, disclosure or use;
    3) processing Users' personal data in accordance with the law;
    4) collecting Users' personal data for specified, lawful purposes;
    5) storing personal data in a form that allows the identification of the data subjects for no longer than is necessary to achieve the purpose of the processing;
    6) processing Users' personal data that is factually accurate and relevant to the purposes for which it is processed.
2. Access to Users' personal data is held by LEAPR and its authorised employees and associates – solely for the purpose and to the extent necessary to provide services using the App. LEAPR may transfer Users' personal data to entities supporting the operation of the App (as described in more detail in sec. VI of the Policy). These entities process data as data processors on the basis of data processing agreements, unless they act as separate data controllers within the scope of a given service (i.e. they independently determine the purposes and means of processing). Analytical and marketing tools are activated in accordance with the User's consent settings in the consent management tool.

IV. Why is Users' personal data processed?

LEAPR processes Users' personal data for the following purposes:

1) the supply of services via the App, i.e. the conclusion and performance of a contract for the supply of electronic services (including the creation and management of an Account, the supply of and participation in Challenges, the tracking of experience points [XP], series and levels, payment processing, subscription management and billing) – (Article 6(1)(b) of the GDPR);
2) providing personalised features of the App and tailoring recommendations to the User's needs: in relation to the analysis of the User's activity and progress necessary for the App to function, pursuant to Article 6(1)(b) of the GDPR; in relation to additional, voluntarily provided data used for personalisation, on the basis of the User's consent, in accordance with Article 6(1)(a) of the GDPR; and to the extent that such data constitutes special categories of personal data, on the basis of the User's voluntary and explicit consent, in accordance with Article 6(1)(a) and Article 9(2)(a) of the GDPR;

3) sending marketing messages and content (depending on the wording of the consent clause for marketing communications – via email or 'push' notifications, as appropriate) on the basis of the User's voluntary consent given whilst using the App (Article 6(1)(a) of the GDPR); irrespective of the GDPR, the sending of commercial information or direct marketing via electronic communication channels (e.g. email, 'push' notifications) may require separate consent in accordance with the provisions of the Electronic Communications Act; such consents are collected and managed separately for each channel;

4) fulfilling the legal obligations incumbent on LEAPR, which arise from the provisions governing the supply of services or LEAPR's activities, as well as provisions relating to customer service, accounting and tax matters (pursuant to Article 6(1)(c) of the GDPR);

5) conducting electronic and traditional correspondence, as well as telephone communications, which constitutes a legitimate interest of LEAPR (pursuant to Article 6(1)(f) of the GDPR); where LEAPR is contacted by telephone regarding matters unrelated to the services provided by LEAPR or any other contract concluded with LEAPR, LEAPR may request personal data only where this is necessary to deal with the matter to which the telephone contact relates, which constitutes a legitimate interest of LEAPR (pursuant to: Article 6(1)(f) of the GDPR);

6) assessing risks and improving the operation of the App, in particular through the analysis of Users' activity, statistics and reporting, and the optimisation of functions and operations, which constitutes a legitimate interest of LEAPR pursuant to Article 6(1)(f) of the GDPR;

7) in accordance with legal requirements, or in connection with ongoing legal proceedings, or in response to a request from a public authority to disclose information held by LEAPR, which constitutes a legitimate interest of LEAPR within the meaning of Article 6(1)(f) of the GDPR, and, in the case of a request from an authorised public authority, to comply with a legal obligation imposed on LEAPR within the meaning of Article 6(1)(c) of the GDPR;

8) ensuring the security of the App and Users, and preventing misuse, which constitutes a legitimate interest of LEAPR within the meaning of Article 6(1)(f) of the GDPR;

9) ensuring that processing complies with personal data protection legislation and LEAPR's internal regulations in this regard, which constitutes a legitimate interest of LEAPR within the meaning of Article 6(1)(f) of the GDPR.

V. How long does LEAPR retain Users' personal data?

1. Personal data will be retained by LEAPR for the period necessary to fulfil the purposes of processing, with this period depending on the purpose and legal basis:

   1) Account data (provided during registration) – for the duration of the supply of services (maintenance of the Account) and for 30 days following its deletion;

   2) data from surveys and questionnaires completed by the User (psychological questionnaire and post-Challenge surveys) – for the duration of the supply of services (maintaining the Account), and deleted upon its deletion;

   3) data relating to activity and progress within the App – for the duration of the provision of services (maintaining the Account) and for 30 days after its deletion;

   4) billing/accounting data – for the period required by Polish accounting and tax legislation;

   5) data processed on the basis of consent (e.g. marketing, 'push' notifications) – until consent is withdrawn;

6) diagnostic and analytical data – for a period of 12 months in a form that allows identification from the time of its collection from the User;

When data is no longer required for the purpose for which it was collected, LEAPR deletes it or renders it irreversibly anonymous.

2. LEAPR states that personal data processed by LEAPR:

   1) for the purposes of direct marketing, will be retained until an objection to the processing of such data is received, and in the case of marketing carried out on the basis of consent to the processing of such data, will be retained until such consent is withdrawn;

   2) for the purpose of fulfilling obligations arising from applicable law (e.g. for the purpose of issuing an invoice) will be retained for the period required by such legislation, e.g. accounting and tax law;

   3) for the purpose of providing services via the App, they will be retained until such time as LEAPR is able to establish, defend or pursue claims – in accordance with the generally applicable limitation periods for claims.

VI. To whom does LEAPR transfer Users' personal data?

1. LEAPR does not share, sell or otherwise disclose the personal data it collects, except in the circumstances described in the Policy or where required by applicable law.

2. LEAPR may transfer Users' personal data to service providers involved in the operation of the App, including (provided that the entities listed below may change; any such changes will be reflected in the then-current version of the Policy):

   1) Google Firebase – for the provision of authentication services, App analytics, crash reports and database management;

   2) Amazon Web Services – for the provision of hosting services and cloud data storage;

   3) RevenueCat – for the provision of subscription and purchase management services;

   4) Apple (APN/Apple App Store) – to enable push notifications and to finalise purchases on the Apple App Store;

   5) Google (Google Play/Play Billing) – for the purpose of finalising purchases on Google Play.

   These entities process data on behalf of LEAPR as data processors (under data processing agreements), unless they act as separate data controllers within the scope of a given service (i.e. they independently determine the purposes and means of processing).

3. Furthermore, LEAPR may disclose data to professional bodies providing services to LEAPR, in particular legal, consultancy, audit, accounting and IT services, to the extent necessary to fulfil the purposes of processing personal data.

4. LEAPR requires these service providers to ensure, in accordance with the law, a high level of privacy and security for the personal data they process on behalf of LEAPR.

5. As a general rule, Users' personal data is not transferred outside the European Economic Area (EEA). However, if, in connection with LEAPR's use of the services of suppliers or their subcontractors, data is transferred outside the EEA or remote access to data from outside the EEA becomes possible (e.g. Google Firebase, RevenueCat), LEAPR will ensure that the transfer complies with the GDPR, in particular on the basis of a European Commission decision confirming an adequate level of protection, Standard Contractual Clauses (SCCs) or another appropriate mechanism, and – where necessary – additional safeguards.

VII. How does LEAPR protect Users' personal data?

1. LEAPR implements appropriate technical and organisational safeguards to ensure an adequate level of protection for personal data, including special categories of personal data.
2. In particular, LEAPR implements:
    1) data encryption during transmission (TLS) and whilst in storage;
    2) an access control system and the principle of least privilege – access by LEAPR employees and associates to special categories of data is restricted;
    3) additional restrictions on access to special categories of data (psychological data and data relating to well-being);
    4) regular security reviews of LEAPR's systems and the practices of data processors acting on LEAPR's behalf.

VIII. What rights do Users have in relation to the processing of their personal data?

1. Within the limits of the law, the User has the right to access their personal data, in particular as a means of monitoring the processing of their personal data by LEAPR, and specifically to obtain information on the purpose, scope and method of data processing.
2. Within the limits of the law, the User also has the right to amend, supplement, rectify and update their personal data processed by LEAPR.
3. Within the limits of the law, the User also has the right to request the erasure of their personal data processed by LEAPR.
4. If the processing of personal data is based on the User's consent, the User has the right to withdraw their consent to the processing of their personal data by notifying LEAPR in any manner. In such situations, LEAPR will comply with the User's decision in relation to future activities, which means that the withdrawal of consent does not affect the lawfulness of the processing carried out prior to the withdrawal of consent.
5. The User has the right – in the cases provided for by law – to request that LEAPR restrict the processing of their personal data.
6. For reasons relating to the User's particular situation and within the limits of the law, the User has the right to object to the processing of their personal data by LEAPR based on the pursuit of its legitimate interests. Notwithstanding the above, the User has the right to object to the processing of data for direct marketing purposes at any time and without giving reasons; once an objection has been lodged, LEAPR will not process the data for that purpose.
7. Within the limits of the law, the User has the right to receive, in a structured, commonly used and machine-readable format, the personal data concerning them that they have provided to LEAPR, and the right to transmit that personal data to another controller without hindrance from LEAPR. However, LEAPR will only do so if such a transfer is technically feasible. The right to data portability applies only to data which LEAPR processes on the basis of a contract concluded with the User or on the basis of the User's consent.
8. These rights may be exercised by sending an email to: **privacy@leapr.app** or by contacting LEAPR in any other manner preferred by the User.

9. If the User considers that LEAPR's processing of personal data infringes the law, they may lodge a complaint with the supervisory authority; in the case of Poland, this is the President of the Personal Data Protection Office.

IX. Can the Privacy Policy be amended?

1. LEAPR may periodically amend the Policy. Such amendments are intended to reflect changes in LEAPR's practices regarding the handling of personal data and to strengthen LEAPR's personal data protection framework.
2. Significant changes to the Policy will be highlighted by means of clearly visible notices displayed within the App and – where appropriate – sent to Users. At the top of the page containing the Policy, you will find information on the date of its most recent update and the date on which the changes come into effect.

X. Is automated decision-making applied to Users' personal data?

No, personal data of Users collected by LEAPR is not subject to automated decision-making within the meaning of Article 20 of GDPR.