

LEGITAM P.S.A.

PRIVACY POLICY — MOBILE APPLICATION

for the Legitam Mobile Application (Android and iOS)

Controller: Legitam Prosta Spółka Akcyjna (a Polish simple joint-stock company, "Legitam P.S.A."), with its registered office at ul. Weselna 5, 46-300 Świercze, Poland.

Application: Legitam Mobile Application (iOS / Android).

Document version: 2.0 / 2026 (supersedes the version dated 10 April 2026)

Effective date: 28 August 2026

Language Versions and Interpretation

These documents are provided in English, Italian, French, Polish, and German for your convenience.

For Consumers: In the event of any material discrepancy between the language versions, the version in the official language of your country of residence (or the language in which you concluded the agreement) shall prevail for the purpose of interpretation, ensuring that your rights under mandatory local consumer protection laws are fully preserved.

For Non-Consumers (B2B): The English version shall be the sole governing and legally binding version for the purpose of interpretation.

In all cases, nothing in this clause shall limit or exclude any mandatory rights granted to you by the applicable law of your country of residence.

Relationship to other documents: This Privacy Policy describes the rules for processing the personal data of Users of the Application, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (the "GDPR"). The rules for using the Application and the services provided through it are set out in the Terms of Service, and the license terms for the software are set out in the End-User License Agreement (EULA). Both documents are available in the Application and at legal.legit.am. Use of the Application requires acceptance of the Terms of Service and the EULA; this Privacy Policy is informational and describes the processing of data in accordance with Article 13 GDPR. The processing of data in connection with the use of the legit.am and privacy.legit.am websites is governed by a separate Privacy Policy — Websites. Our approach to combating child sexual abuse and exploitation, including the related processing of data, is set out in the Child Safety Standards (CSAE).

§1. DATA CONTROLLER

The controller of the personal data of Users of the Application within the meaning of the GDPR is:

Company:	Legitam P.S.A.
Address:	ul. Weselna 5, 46-300 Świercze, Poland
E-mail:	privacy@legit.am
Data Protection Officer (DPO):	dpo@legit.am
Effective date:	28 August 2026

§2. SCOPE OF DATA COLLECTED

2.1. Registration data

- first name / surname or username (nickname);
- e-mail address and password (stored in encrypted form);
- profile picture (optional);
- date of birth (used to verify the minimum age of 16).

2.2. User-generated content

- amLooks — posts, photos, videos, and other media;
- comments and ratings on other Users' content;
- contents of the Digital Closet (products assigned via NFC Tags).

2.3. Data from NFC Tags

When a physical NFC Tag embedded in a product is scanned, we collect:

- the unique NFC Tag identifier;
- the date and time of the scan;
- the geographic location at the time of scanning — solely with the User's consent;
- information about the associated physical item;
- Digital Product Passport (DPP) data — supplied by the manufacturer; the Application only displays it.

2.4. Behavioural and activity data

- browsing and interaction history;
- ratings and comments;
- NFC scan history;
- activity within the Digital Closet;
- data used to calculate the AmRank indicator.

2.5. Device technical data

- device identifier (Device ID);
- operating system and Application version;
- IP address;
- diagnostic and error logs;
- advertising identifiers (IDFA / GAID) — solely with the User's consent.

2.6. Moderation and report data

- the content of reports and appeals and the reporting person's contact details (if provided);
- content reported, blocked or removed as a result of moderation;
- moderation decisions, the statements of reasons and the measures applied;
- correspondence with the User concerning reports, complaints and appeals.

Providing the registration data (§2.1) is voluntary but necessary to conclude the contract and create an Account — without it, an Account cannot be created. Providing other data is voluntary; refusing consent to location access, analytics or the use of advertising identifiers does not restrict the basic features of the Application.

§3. PURPOSES AND LEGAL BASES FOR PROCESSING

3.1. Performance of a contract — Article 6(1)(b) GDPR

- registration and Account administration;
- publishing content and social interactions (amLooks, comments, follows, groups);
- operating the Digital Closet;
- displaying DPP data upon scanning an NFC Tag.

3.2. Legitimate interest of the controller — Article 6(1)(f) GDPR

- calculating the AmRank indicator (an algorithm that constitutes a trade secret of Legitam P.S.A.);
- personalising the content feed based on User activity;
- security and integrity of the Application, including detecting abuse of scanning features;
- server-side statistics and error reports necessary to maintain and improve the quality of the services.

3.3. User consent — Article 6(1)(a) GDPR

- access to the device's geographic location at the time an NFC Tag is scanned;
- analytics of the use of the Application based on data stored on or read from the device (analytics tools), to the extent going beyond what is strictly necessary;
- use of advertising identifiers (IDFA / GAID).

3.4. Legal obligation — Article 6(1)(c) GDPR

- retention of data required under tax and accounting regulations.

3.5. Content moderation and safety — Article 6(1)(c) and (f) GDPR

- handling reports, taking and stating the reasons for moderation decisions and handling appeals — obligations under Articles 16, 17 and 20 of Regulation (EU) 2022/2065 (DSA);
- combating illegal content, including preserving CSAM and reporting it to law enforcement as described in §11–12 of the Child Safety Standards (CSAE);
- establishing, exercising or defending legal claims.

§4. NFC TAGS, DPP, AND AUTHENTICITY VERIFICATION

4.1. NFC Tags embedded in products enable an item to be assigned to an Account, the DPP to be displayed, and the scan data described in §2.3 to be recorded.

4.2. DPP data is supplied solely by manufacturers or brands. In this regard, Legitam P.S.A. acts as a technical intermediary displaying this information and bears no responsibility for its content, accuracy, or currency.

4.3. Authenticity verification — disclaimer. Legitam P.S.A. takes all reasonable steps to ensure the reliability of product-authenticity verification via NFC Tags. However, due to continuing technological developments, Legitam P.S.A. cannot rule out that instances of false readings (NFC spoofing or other forms of interference) may occur in the future. Legitam P.S.A. bears no liability for damages arising from such events, provided it has exercised due diligence with respect to the security measures applied.

§5. THE AMRANK INDICATOR

Every User is assigned an AmRank indicator, calculated based on the verified value of their Digital Closet and their level of community engagement (including creating amLooks and rating other Users). The calculation algorithm

constitutes a trade secret and intellectual property of Legitam P.S.A. A User may ask Legitam P.S.A. about the general criteria affecting the indicator but is not entitled to obtain details of the algorithm.

Calculating AmRank and personalising the feed constitute profiling within the meaning of Article 4(4) GDPR. No decisions producing legal effects concerning the User or similarly significantly affecting them are taken on that basis (Article 22 GDPR); moderation decisions are taken with human involvement (§7.2 of the Terms of Service). The User may object to profiling based on legitimate interest (Article 21 GDPR).

§6. DISCLOSURE OF DATA TO OTHER PARTIES

6.1. Processors (Article 28 GDPR)

- Amazon Web Services (AWS) — server infrastructure and data storage;
- analytics and diagnostics service providers;
- payment service providers (where applicable).

6.2. Public authorities

Data may be disclosed to authorised authorities solely to the extent required by applicable law.

6.3. Transfers outside the European Economic Area (EEA)

Data is stored on AWS servers. Transfers of data outside the EEA are safeguarded by Standard Contractual Clauses (SCCs) approved by the European Commission.

6.4. Other Users

Content published by the User (amLooks, comments) and profile data (username, profile picture, AmRank) are visible to other Users of the Application to the extent resulting from its features and the User's settings (e.g., audience groups).

§7. SECURITY AND DATA RETENTION PERIODS

7.1. Security measures

- encryption of data in transit (TLS/HTTPS);
- password encryption (hashing);
- access controls for systems and data;
- regular security audits.

7.2. Retention periods

- Account data: for the duration of the Account. Once a request to delete the Account has been submitted, data is processed to a limited extent during the 30-day blocking period described in the Terms of Service (§3.3–3.4 of the Terms of Service), after which it is permanently deleted or anonymised;
- data required under tax and accounting regulations: for the period required by such regulations (generally 5 years, counted from the end of the tax year in which the tax obligation arose);
- User Content (amLooks, comments): until deleted by the User or until the Account is deleted;
- NFC Tag data: until consent is withdrawn (for data based on consent, e.g. location) or until the Account is deleted;
- data used to calculate AmRank: for the duration of the Account;
- reports, moderation decisions and appeals: for the time needed to handle them and then for 6 months — the period for lodging an appeal (§7.4 of the Terms of Service);

- content blocked or removed as a result of moderation or a report: 6 months from blocking, unless longer retention is required by law or requested by law enforcement (§11 of the Child Safety Standards);
- technical and diagnostic logs: up to 12 months.

§8. USER RIGHTS

Under the GDPR, the User has the following rights:

- the right of access to data — Article 15 GDPR;
- the right to rectification of data — Article 16 GDPR;
- the right to erasure of data (“the right to be forgotten”) — Article 17 GDPR;
- the right to restriction of processing — Article 18 GDPR;
- the right to data portability — Article 20 GDPR;
- the right to object to processing — Article 21 GDPR;
- the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects the User — Article 22 GDPR;
- the right to withdraw consent at any time, without affecting the lawfulness of processing carried out before its withdrawal — Article 7(3) GDPR.

Requests concerning the exercise of the above rights should be directed to the Data Protection Officer at dpo@legit.am. Legitam P.S.A. will respond without undue delay, and in any event within one month of receiving the request.

The User has the right to lodge a complaint with the supervisory authority — the President of the Personal Data Protection Office, ul. Stawki 2, 00-193 Warsaw, Poland.

In accordance with Article 77 GDPR, the User may also lodge a complaint with the supervisory authority of the Member State of their habitual residence or place of work, in particular: in France — the Commission Nationale de l'Informatique et des Libertés (CNIL, www.cnil.fr); in Germany — the data protection authority of the federal state (Land) in which the User resides, or the Federal Commissioner for Data Protection and Freedom of Information (BfDI, www.bfdi.bund.de); in Italy — the Garante per la protezione dei dati personali (www.garanteprivacy.it).

§9. CHILDREN'S DATA

The Application is not intended for persons under the age of 16, in accordance with the registration requirement set out in the Terms of Service. Legitam P.S.A. does not knowingly collect data from persons under this age. Data collected without the required consent or age verification will be deleted promptly upon becoming aware of it.

§10. COOKIES AND TRACKING TECHNOLOGIES

The Application uses local data storage and device identifiers to the extent strictly necessary to provide the service (maintaining sessions, remembering preferences, error diagnostics and security) and otherwise — including for analytics and the use of advertising identifiers — only with the User's consent, which may be withdrawn at any time. Users manage the Application's permissions (including access to location and advertising identifiers) in their iOS / Android system settings. The use of cookies on Legitam's websites is governed by a separate Cookie Policy.

§11. CHANGES TO THIS PRIVACY POLICY

Legitam P.S.A. will provide at least 14 days' advance notice of any material changes to this Privacy Policy, via a push notification, e-mail, or an in-app message shown after login. Where a change requires the User's consent (e.g., a new purpose of processing based on consent), Legitam P.S.A. will request it separately.

§12. CONTACT

Controller:	Legitam P.S.A., ul. Weselna 5, 46-300 Świercze, Poland
E-mail (privacy, Account):	privacy@legit.am
Account deletion request:	privacy.legit.am
Data Protection Officer:	dpo@legit.am
Supervisory authority:	President of the Personal Data Protection Office (UODO), ul. Stawki 2, 00-193 Warsaw, Poland
Effective date:	28 August 2026

This Privacy Policy (Mobile Application) is effective as of 28 August 2026 | Compliant with the GDPR (Regulation (EU) 2016/679) | Legitam P.S.A.