MUYA PRIVACY POLICY

Version 1.0 | Effective as of 15.05.2026

1. Introduction and General Information

This Privacy Policy sets out the rules for the processing of personal data of persons using the website www.muya.app (hereinafter: the "Website"), the MUYA mobile application (hereinafter: the "Application"), and the newsletter service operated by the Data Controller.

This document has been prepared in accordance with the requirements of 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 (hereinafter: "GDPR"), as well as taking into account local provisions applicable in the jurisdictions in which the Application is available (details in Section 16).

Please read this Policy carefully. Using the Website, the Application, or subscribing to the newsletter constitutes acceptance of the rules described in this document. For matters related to the protection of personal data, please contact us at: hi@muya.app.

2. Data Controller

The data controller within the meaning of Art. 4(7) GDPR is Sopraya Sp. z o.o. **with its registered office in Chodzież (64-800), ul. Krasińskiego 20, entered in the register of entrepreneurs of the National Court Register maintained by the District Court Poznań - Nowe Miasto i Wilda in Poznań, 9th Commercial Division, under KRS number 0001165422, NIP 6070098148, REGON 541318039.**

Data Controller contact details:

- email address (GDPR and data protection matters): hi@muya.app
- email address (complaints): contact@sopraya.com
- phone: +48 660 927 243
- correspondence address: ul. Krasińskiego 20, 64-800 Chodzież, Poland

The Data Controller has not appointed a Data Protection Officer (DPO), as the scale and nature of the data processed do not require such appointment under Art. 37 GDPR. For all matters concerning the processing of personal data, please contact us at hi@muya.app.

3. Definitions

For the purposes of this Policy, the following terms shall have the meanings set out below:

- **Data Controller** - Sopraya Sp. z o.o. as described in Section 2.
- **Website** - the website available at www.muya.app, including the blog and newsletter sign-up form.

- **Application** - the MUYA mobile application available for iOS devices (App Store) and Android devices (Google Play).
- **User** - a natural person who is at least 16 years of age and uses the Website, the Application, or the newsletter.
- **B2C User** - an individual User who purchased a subscription directly through the App Store or Google Play.
- **B2B User** - a User who obtained access to the Application through a corporate subscription granted by their employer (Organisation).
- **Organisation** - an entity (business) that has entered into a B2B agreement with the Data Controller for access to the Application for its employees or collaborators.
- **Personal data** - any information relating to an identified or identifiable natural person, within the meaning of Art. 4(1) GDPR.
- **Processing** - any operation performed on Personal data, within the meaning of Art. 4(2) GDPR.
- **Sub-processor** - a third party providing technical, analytical, or marketing services to the Data Controller, to whom the Data Controller entrusts the processing of personal data under an appropriate agreement.
- **Newsletter** - a service of free, periodic dispatch of electronic messages containing commercial and marketing information about the Data Controller's activities.

4. Scope of Application of this Policy

This Policy covers the processing of data in the following areas:

- **Website www.muya.app** - an informational website with a blog and newsletter sign-up form. The Website is of a presentational and marketing nature.
- **Newsletter** - a service for sending marketing messages, operated through the sign-up form on the Website and (optionally) in the Application.
- **MUYA mobile application - B2C model** - use of the Application by individual Users who have purchased a subscription themselves.
- **MUYA mobile application - B2B model** - use of the Application by Users to whom access has been granted by an employer (Organisation) under a B2B agreement.

This Policy applies globally. The Application is available in 6 language versions (Polish, English, German, Italian, Spanish, French) and may be used by Users from any country, subject to the local provisions described in Section 16. Additional language versions (including Japanese) will be made available as part of subsequent stages of product development, together with the corresponding versions of this Privacy Policy.

5. Legal Roles of the Data Controller

Depending on the model of use of the Application, Sopraya Sp. z o.o. acts in different legal roles:

5.1. B2C Model - Data Controller

With respect to individual (B2C) Users, Website users, and newsletter subscribers, Sopraya Sp. z o.o. acts as data controller within the meaning of Art. 4(7) GDPR - independently determining the purposes and means of processing.

5.2. B2B Model - Data Processor

With respect to B2B Users whose data (in particular email addresses) have been provided to the Data Controller by the Organisation for the purpose of granting access to the Application, Sopraya Sp. z o.o. acts as data processor (Art. 28 GDPR) on behalf of the Organisation. In this scope, the Data Controller processes personal data exclusively in accordance with the instructions set out in the Data Processing Agreement (DPA) concluded with the Organisation.

Independently of the above, from the moment a User creates an Account and accepts the Terms of Service, Sopraya Sp. z o.o. also acts as an independent data controller with respect to data processed for its own purposes (e.g. ensuring the security of the Application, pursuing claims).

In the event that the alternative B2B model based on B2B Activation Codes is launched in the future, Sopraya Sp. z o.o. will act exclusively as an independent data controller with respect to data provided directly by the User when creating the Account, as the Organisation will not transfer any personal data to the Data Controller in that model.

6. Categories of Personal Data Processed

6.1. Data Collected on the Website (www.muya.app)

- IP address of the User's device
- cookie identifiers and similar technology identifiers
- device and browser information (User-Agent, operating system, screen resolution, language)
- the page from which the User arrived at the Website (referrer)
- data about the User's behaviour on the Website (pages visited, session duration, interactions) - collected via Google Analytics 4 (after obtaining consent)
- data on interactions with advertisements and conversion events (clicks on Google and Meta ads) - collected via Google Ads and Meta Pixel (after obtaining consent)
- advertising identifiers used for remarketing (Google Ads Remarketing, Meta Pixel) - processed exclusively after obtaining User consent

6.2. Data Collected upon Newsletter Sign-up

- email address
- first name (optional, if the form includes such a field)
- date and time of sign-up in the form, IP address, and session identifier (for evidentiary purposes)

- date and time of consent confirmation by clicking the activation link sent to the email address (double opt-in mechanism)
- analytical data on interactions with the newsletter (email opens, link clicks) - processed by MailerLite

6.3. Data Collected in the Application - Identification and Account

- email address (primary Account identifier)
- first name (optional; may originate from Apple Sign-In or Google Sign-In login or be entered by the User)
- user identifier in the Clerk system (identity management service, which is the primary authentication provider)
- hashed Apple ID or Google account identifier (in the case of login via Apple Sign-In or Google Sign-In)
- JWT session tokens (stored locally on the device)

6.4. Technical Application Data

- device identifier (on iOS: IDFV - Identifier for Vendor; on Android: Firebase Installation ID)
- operating system, system version, Application version
- Application language and time zone
- IP address (recorded in Cloudflare logs and application logs)
- Cloudflare Workers application logs - recorded technical events (exceptions, server errors, API response times) - stored for up to 12 months
- crash and error data from the Application (stack traces, Application and device state at the time of the error) - collected in the production version by Firebase Crashlytics upon consent

6.5. Usage (Behavioural) Data in the Application

- history of played audio sessions (recordings, date, playback duration)
- favourite sessions
- session start and end times
- analytical events (screen opens, clicks on CTA elements), user identifier and user properties (account type, subscription level, Application language and theme, login provider) - processed by Firebase Analytics upon consent in the Application

6.6. Subscription and Transaction Data

- subscription status (free / active / expired)
- plan type (monthly / annual)
- purchase date and subscription expiry date

- transaction identifier (App Store / Google Play / promotional subscription / activation code)
- subscription source (B2C - App Store or Google Play; B2B - assignment by Organisation; promotional code)
- data related to the use of Promotional Codes (code identifier, activation date, code type)

The Data Controller does not store payment card numbers or other payment data - transactions are processed directly by App Store or Google Play.

6.7. Additional Data in the B2B Model

- Organisation (employer) name
- invoice number
- corporate subscription validity period
- association of the User's email address with the Organisation
- activation code batch identifier (in the codes model)
- Organisation's Contact Person data (first name, surname, email, position) - to the extent necessary for contract performance
- Organisation's billing data (VAT number, address, invoice details)

6.8. What We Do NOT Collect

The Data Controller declares that, within the Website and Application:

- it does not collect medical data or data concerning Users' health status
- it does not collect special categories of data within the meaning of Art. 9 GDPR (including biometric, genetic, health, or data revealing racial or ethnic origin)
- it does not collect data of children under the age of 16 (details in Section 15)
- it does not store passwords - authentication is handled by Clerk, with support for Apple Sign-In and Google Sign-In
- it does not use the App Tracking Transparency (ATT) mechanism - it does not track Users across other companies' apps and websites

6.9. Data of Creators and Promotional Partners

Within partner programmes and collaborations with Creators (influencers), the Data Controller processes the following data of Creators:

- identification and contact data (full name or business name, email address, phone number)
- billing data (VAT number, business address, bank account number, invoice details)
- collaboration data (Creator identifier, assigned Promotional Codes, campaign identifier, conversion statistics)

- settlement data (amount of commissions due, number of successful conversions, settlement dates)
- social media information of the Creator (username, profile link) - solely in the scope necessary for campaign management

7. Purposes and Legal Bases for Processing

Personal data are processed for the following purposes, on the following legal bases:

7.1. Provision of Services (Account management, delivery of audio content, subscription handling)

Legal basis: Art. 6(1)(b) GDPR - processing necessary for the performance of a contract to which the User is a party (Terms of Service), or in order to take steps at the request of the User prior to entering into a contract.

7.2. Sending of Newsletter and Marketing Communications

Legal basis: Art. 6(1)(a) GDPR - voluntary consent of the User, as well as Art. 10 of the Act on Providing Services by Electronic Means [provision based on Polish law] - for sending commercial information by electronic means.

Double opt-in mechanism: newsletter sign-up takes place through a two-step confirmation model: (1) the User enters their email address in the form; (2) a confirmation email is sent, and the subscription is activated only after the User clicks the activation link.

Withdrawal of consent: consent may be withdrawn at any time by clicking the "Unsubscribe" link in any newsletter email, or by contacting the Data Controller at hi@muya.app. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

7.3. Analytics, Diagnostics and Product Development (GA4 on Website, Firebase in Application)

Legal basis: Art. 6(1)(a) GDPR - consent expressed in the cookie consent banner (for the Website) or in the consent prompt upon the first launch of the Application or in the Application settings (for the Application), with the option to withdraw at any time. Until consent is given, analytics and diagnostics in the Application remain disabled.

7.4. Marketing, Advertising, and Remarketing (Meta Pixel, Google Ads)

Legal basis: Art. 6(1)(a) GDPR - User consent expressed in the cookies consent banner.

Scope of marketing activities: the Data Controller runs advertising campaigns in the Meta ecosystem (Facebook, Instagram) and Google ecosystem (Google Search, Display Network, YouTube) using tools such as Meta Pixel and Google Ads. These campaigns target potential new Users and, where consent has been granted, existing Users (remarketing).

Newsletter: the Data Controller does not pass newsletter subscribers' email addresses to Meta, Google, or other advertising platforms for the purpose of creating custom audiences or running campaigns targeted at subscribers.

Withdrawal of consent: consent to marketing cookies may be withdrawn at any time through the cookie settings available in the Website footer. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

7.5. Payment Processing and Settlements

Legal basis: Art. 6(1)(b) GDPR (performance of contract) and Art. 6(1)(c) GDPR (legal obligation) - in the scope of issuing invoices and complying with tax law requirements.

7.6. Handling of Contact Enquiries and Complaints

Legal basis: Art. 6(1)(b) GDPR (actions at the request of the data subject prior to entering into a contract or performance of contract) and Art. 6(1)(f) GDPR (legitimate interest of the Data Controller in handling correspondence and resolving complaints).

7.7. Ensuring the Security of the Website and Application; Fraud Prevention

Legal basis: Art. 6(1)(f) GDPR - legitimate interest of the Data Controller consisting in ensuring the security of IT systems, detecting and preventing abuse, and maintaining system integrity.

7.8. Pursuit and Defence of Claims

Legal basis: Art. 6(1)(f) GDPR - legitimate interest of the Data Controller consisting in the ability to establish, pursue, or defend legal claims.

7.9. B2B Settlements (Organisation and Contact Person Data)

Legal basis: Art. 6(1)(b) GDPR (performance of the B2B Agreement), Art. 6(1)(c) GDPR (legal obligation - issuing invoices, tax obligations), Art. 6(1)(f) GDPR (legitimate interest in B2B settlements).

7.10. Processing of Organisation Employees' Data on behalf of the Organisation (B2B)

Legal basis: Art. 28 GDPR - entrustment of processing on the basis of a separate DPA agreement concluded between the Data Controller and the Organisation. In this scope, Sopraya Sp. z o.o. acts as data processor and processes data solely in accordance with the Organisation's instructions.

7.11. Collaboration with Creators and Promotional Partners (Partner Programmes)

Legal basis: Art. 6(1)(b) GDPR (performance of the agreement concluded with the Creator), Art. 6(1)(f) GDPR (legitimate interest in running partner programmes and settling commissions).

Providing personal data is voluntary, but necessary for creating an Account, purchasing a subscription, signing up for the newsletter, or entering into collaboration as a Creator. Without providing the required data, it will not be possible to use the relevant service.

8. Sub-processors and Data Recipients

The Data Controller uses trusted external service providers who may process personal data on its behalf. The current list of sub-processors is as follows:

8.1. Cloudflare, Inc. (USA)

- **Scope of services:** hosting of the Application API (Cloudflare Workers), audio file storage (Cloudflare R2), CDN, DDoS protection, WAF (Web Application Firewall).
- **Data processed:** email address, user identifier, session tokens, access logs, IP addresses, technical event logs.
- **Location:** global edge infrastructure. Transfer to the USA secured by Standard Contractual Clauses (SCC) and EU-US Data Privacy Framework (DPF).

8.2. DigitalOcean, LLC (Frankfurt, EU)

- **Scope of services:** managed PostgreSQL database.
- **Data processed:** full set of User Account data, subscriptions, audio session history, B2B organisational data.
- **Location:** Frankfurt, Germany (EEA).

8.3. Apple Inc. (USA / EU)

- **Scope of services:** login via Apple Sign-In (SSO), B2C payment processing via App Store.
- **Data processed:** email address, first name, hashed Apple ID identifier, transaction data.
- **Location:** USA and EU. Transfer to the USA secured by SCC and DPF.

8.4. Google LLC (USA / EU)

- **Scope of services:** B2C payment processing via Google Play (Android), login via Google Sign-In, Firebase Analytics, Google Analytics 4, Google Ads.
- **Data processed:** device identifier, telemetry data, transaction data, email address, usage events and Application crash data (Firebase Crashlytics). The advertising identifier applies exclusively to the Website (Google Ads) - the Application does not collect advertising identifiers.
- **Location:** USA and EU. Transfer to the USA secured by SCC and DPF.

8.5. RevenueCat, Inc. (USA)

- **Scope of services:** management of User subscriptions and entitlements, synchronisation of subscription status across platforms (App Store, Google Play, B2B).
- **Data processed:** email address, User identifier (appUserId), payment history, subscription status.
- **Location:** USA. Transfer secured by SCC and DPF.

8.6. Clerk, Inc. (USA)

- **Scope of services:** user identity management service (authentication and user management), handling of login via email, Apple Sign-In, Google Sign-In.
- **Data processed:** email address, first name, User identifier, session metadata (IP address, User-Agent, device identifier).
- **Location:** USA. Transfer secured by SCC and DPF.

8.7. Firebase (Google Ireland Limited / Google LLC)

- **Scope of services:** analytics and statistics of mobile Application usage (Firebase Analytics), stability monitoring and crash reporting (Firebase Crashlytics) and installation identifier assignment (Firebase Installations). In the future - push notifications (functionality will be activated in a future version of the Application).
- **Firebase Analytics and Crashlytics are disabled by default and activated only upon the User voluntarily consenting in the Application (consent prompt upon first launch) or in the Application settings. Consent may be withdrawn at any time in the Application settings; withdrawal stops further data collection and removes the installation identifier from the device, but does not cover data already transmitted to Google before withdrawal (stored until the retention period expires). Firebase Analytics operates on Android devices; on iOS devices it remains disabled in the Application configuration.**
- **Data processed:** usage events (including screen openings, audio session playback, subscription and gift code events) with parameters; user properties (account type, subscription level, Application language and theme, login provider); user identifier and Firebase Installation ID (Android devices); automatic SDK data on Android (device model and system, Application version, session data); for Crashlytics - Application crash and error data (stack traces, Application and device state at the time of the error) linked to the user identifier.
- **The Application does not use the advertising module (AdMob) and does not collect advertising device identifiers (IDFA / GAID); Firebase data is not used for advertising or remarketing.**
- **Legal basis:** Art. 6(1)(a) GDPR - User consent expressed in the Application.
- **Location:** USA and EU. Transfer to the USA secured by Standard Contractual Clauses (SCC) and under the EU-US Data Privacy Framework (DPF) - Google LLC is a DPF-certified entity.

8.8. MailerLite Limited (Ireland, EU)

- **Scope of services:** newsletter dispatch, subscriber list management, open and click analytics.
- **Data processed:** email address, first name (if provided), sign-up date, IP address, interaction data (opens, clicks).
- **Location:** Ireland (EEA). MailerLite may use sub-contractors outside the EEA - details available at: https://www.mailerlite.com/legal/data-processing-agreement.

8.9. Google Analytics 4 (Google LLC)

- **Scope of services:** traffic analytics on the Website www.muya.app.
- **Data processed:** anonymised IP address, cookie identifiers, device and browser data, behavioural data on the Website.
- **Location:** USA and EU. Transfer secured by SCC and DPF. Activated only after obtaining User consent via the cookies consent banner.

8.10. Meta Platforms Ireland Limited (Meta Pixel, Meta Ads)

- **Scope of services:** measuring the effectiveness of advertising campaigns on Meta platforms (Facebook, Instagram), running remarketing campaigns.
- **Data processed:** cookie identifiers, IP address, data on events on the Website, advertising identifiers.
- **Location:** Ireland and USA. Transfer to the USA secured by SCC and DPF. Meta Pixel is activated only after obtaining User consent.
- **Newsletter data:** the Data Controller does not pass Meta any email addresses or other personal data of Newsletter subscribers for the purpose of creating custom audiences.

8.11. Google Ads (Google Ireland Limited / Google LLC)

- **Scope of services:** running Google Ads campaigns in the Google search engine, Display Network, and YouTube; remarketing.
- **Data processed:** cookie identifiers, advertising identifiers, IP address, data on events on the Website.
- **Location:** Ireland and USA. Transfer to the USA secured by SCC and DPF. Google Ads is activated only after obtaining User consent.

The current list of sub-processors is available in this Policy. The Data Controller informs Users of any planned changes to the list of sub-processors and provides the Organisation (in the B2B model) with the opportunity to object to such changes in accordance with the terms of the DPA.

Personal data may also be disclosed to:

- entities providing accounting, legal, and advisory services to the Data Controller (on the basis of data entrustment agreements)

- public authorities or other authorised entities - exclusively on the basis of applicable legal provisions
- in the B2B model - the Organisation, exclusively in the scope of billing and statistical data specified in the DPA

9. Data Transfers Outside the European Economic Area

Some of the Data Controller's sub-processors are based outside the European Economic Area (EEA), in particular in the USA. Data transfers to third countries are secured by the following mechanisms:

- Standard Contractual Clauses (SCC) approved by the European Commission under Art. 46(2)(c) GDPR
- EU-US Data Privacy Framework (DPF) - for entities certified under this programme (Cloudflare, Google, Meta, RevenueCat, Clerk, Apple)
- additional technical and organisational measures (encryption in transit and at rest, access restriction to minimum necessary scope)

The User has the right to obtain a copy of the security measures applied by contacting the Data Controller at hi@muya.app.

By using the Website or Application, the User acknowledges that their data may be transferred to countries outside the EEA, which are considered to ensure an adequate level of data protection by the mechanisms described above.

10. Data Retention Periods

Personal data are retained for the period necessary to achieve the purposes for which they were collected, and thereafter for the period required by applicable law or justified by the legitimate interests of the Data Controller.

10.1. User Account Data (B2C)

Account data are retained for the entire period of use of the Application. After initiating the account deletion process:

- immediately upon the deletion request - the Account is deactivated and inaccessible to the User
- after 30 days from initiating deletion - a scheduled task (cron) performs a permanent (hard-delete) deletion of all Account data from the production database

After hard-delete, data may remain exclusively in infrastructure backups, for technical reasons, for a maximum period of 90 days, after which they are permanently deleted.

10.2. B2B User Data

User-to-Organisation assignment data are retained for the duration of the corporate subscription. After its expiry or upon the User's Account being removed from the

Organisation's pool, the data are deleted in accordance with the procedure described in Section 10.1, unless the DPA provides otherwise.

10.3. Billing Data and Invoices

Data necessary for issuing invoices and tax settlements (including B2B Organisation data and B2C transaction data) are retained for 5 years from the end of the calendar year in which the tax obligation arose, in accordance with tax law requirements.

10.4. Newsletter Subscriber Data

The email address and related data are retained until consent is withdrawn (unsubscription) or until the newsletter service is discontinued.

In the event of failure to confirm sign-up under the double opt-in mechanism (no activation link click within 7 days), the data are deleted automatically.

10.5. Analytical and Marketing Data (Google Analytics 4, Google Ads, Meta Pixel, Firebase)

Analytical and marketing data are stored for a period consistent with the configuration of the services: Google Analytics 4 (Website) - configured user-level data retention period of up to 14 months; Firebase Analytics (Application) - configured data retention period of up to 14 months; Firebase Crashlytics (Application crash reports) - crash data (stack traces, diagnostic data, installation identifiers) for 90 days, after which they are deleted from production systems and backups; Google Ads (conversion and remarketing cookies) - up to 540 days in accordance with Google's policy; Meta Pixel - in accordance with Meta's policy, usually up to 2 years. Data is deleted earlier if the User withdraws consent in the cookie banner or in the Application settings.

10.6. Technical Data and System Logs

Cloudflare logs and other system logs are retained for a period of up to 12 months, after which they are automatically deleted.

10.7. B2B Activation Codes

Information on generated and used activation codes is retained for 5 years from the date of generation, for evidentiary and settlement purposes.

10.8. Data Related to Handling of Complaints and Enquiries

Contact correspondence data are retained for the period necessary to respond to the enquiry and, if a complaint or dispute arises, for the period necessary to resolve it and until the expiry of the limitation period for claims.

10.9. Data Processed for Claims Purposes

To the extent that processing is necessary for establishing, pursuing, or defending claims, personal data are retained for a period equal to the limitation period for such claims, i.e. up to

6 years from the date on which the claim became due (in accordance with the Civil Code), plus an additional 1 year to account for claims lodged near the end of the limitation period.

11. Rights of Data Subjects

Under the GDPR, the User has the following rights:

- **Right of access (Art. 15 GDPR)** - to obtain confirmation of whether the Data Controller is processing data concerning the User and, if so, to receive a copy of those data together with information on the processing.
- **Right to rectification (Art. 16 GDPR)** - to request the correction of inaccurate data or the completion of incomplete data.
- **Right to erasure ("right to be forgotten", Art. 17 GDPR)** - to request the deletion of data where, for example, they are no longer necessary for the purposes for which they were collected, consent has been withdrawn, or the data have been unlawfully processed.
- **Right to restriction of processing (Art. 18 GDPR)** - to request a temporary suspension of data processing, for example while verifying the accuracy of data or during consideration of an objection.
- **Right to data portability (Art. 20 GDPR)** - to receive data in a structured, commonly used, machine-readable format and to transmit those data to another controller.
- **Right to object (Art. 21 GDPR)** - to object to processing based on the legitimate interests of the Data Controller (Art. 6(1)(f) GDPR), including profiling. The Data Controller shall cease processing unless it demonstrates compelling legitimate grounds which override the interests, rights, and freedoms of the User.
- **Right to withdraw consent** - at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Withdrawal of consent to the newsletter results in removal from the mailing list. Withdrawal of consent to analytical cookies results in the deactivation of GA4/Firebase.
- **Right to lodge a complaint with a supervisory authority** - in Poland: the President of the Personal Data Protection Office (UODO), ul. Stawki 2, 00-193 Warsaw, www.uodo.gov.pl. Users from other countries may lodge a complaint with the competent supervisory authority in their country of residence.

To exercise the above rights, please contact us at hi@muya.app. The Data Controller will respond to requests within the timeframes set out in the GDPR (generally within one month, with the possibility of extending this period by a further two months in complex cases).

In the B2B model, if the request concerns data processed by the Data Controller in the role of data processor on behalf of the Organisation, the Data Controller will forward such request to the Organisation as the data controller and will assist in its handling in accordance with the DPA.

12. Cookies and Similar Technologies on the Website

The website www.muya.app uses cookies and similar technologies (web storage, pixels). Cookies are small text files stored on the User's device when visiting the Website.

12.1. Types of Cookies Used

- **Essential cookies (technical)** - enable the correct operation of the Website (e.g. handling forms, maintaining session). These cookies do not require User consent.
- **Analytical cookies** - used to collect statistics on Website usage (Google Analytics 4). Activated only with User consent.
- **Marketing cookies** - used for marketing activities, including remarketing (Meta Pixel, Google Ads). Activated only with User consent.

12.2. Cookie Consent Management

On first visiting the Website, the User sees a cookies consent banner (Consent Management Platform - CMP). The User may:

- accept all cookies
- reject all optional cookies (only essential cookies remain active)
- make an individual selection of cookie categories

Consent may be modified or withdrawn at any time through the settings available in the Website footer. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

13. Local Technologies in the Mobile Application

The MUYA mobile application does not use cookies in the traditional sense. Within its operation, it uses the following local storage technologies:

- session tokens (JWT) - enabling maintenance of the User's logged-in session
- cache (temporary storage) - used for temporarily storing audio content and interface data to improve Application performance
- Firebase Analytics SDK - for collecting analytical events; Firebase Crashlytics SDK - for reporting Application crashes and errors. Both disabled by default, activated only upon consent in the Application and disabled upon its withdrawal.
- payment provider SDKs (App Store / Google Play) - native operating system components handling subscription verification; these do not store payment card data in the Application

The Application does not use the App Tracking Transparency (ATT) mechanism within the meaning of Apple's policy - it does not track Users across other companies' apps or websites.

14. Data Security

The Data Controller applies technical and organisational measures ensuring the security of data appropriate to the level of risk, including in particular:

- communication encryption (TLS) across the entire network infrastructure (Cloudflare)
- data-at-rest encryption in the PostgreSQL database managed by DigitalOcean
- authentication is handled by Clerk as the primary identity provider, with support for multi-factor authentication (MFA) for administrative users
- versioned JWT session tokens - enabling remote session revocation
- restriction of access to the administration panel exclusively to authorised Data Controller employees
- regular software updates and security reviews
- security incident response procedures and the obligation to notify data breaches to the supervisory authority within 72 hours of becoming aware of them (Art. 33 GDPR)

15. Protection of Minors' Data

The Website and Application are not intended for persons under the age of 16. The Data Controller does not knowingly collect personal data from persons under the age of 16.

The Data Controller applies a uniform, elevated threshold of 16 years worldwide, regardless of local provisions applicable in individual jurisdictions (e.g. the United Kingdom - 13 years, Ireland - 13 years, certain EU Member States - 13 or 14 years). This decision results from the wellness nature of the Application and the aim of maintaining a consistent and transparent policy for the protection of minors.

When creating an Account, the User declares that they are at least 16 years of age. Should the Data Controller become aware that personal data of a person under the age of 16 has been collected, such data will be immediately deleted and the Account will be blocked.

Parents or legal guardians who suspect that a child under the age of 16 has provided the Data Controller with their personal data are requested to contact us at hi@muya.app. The Data Controller will promptly delete such data.

16. Local Provisions in Selected Jurisdictions

The Application is available globally. In addition to the rights granted to Users under the GDPR, the following additional rights or obligations may apply depending on the User's country of residence:

16.1. United Kingdom (UK GDPR and Data Protection Act 2018)

UK GDPR and the Data Protection Act 2018 apply to Users in the United Kingdom. The rights of UK Users are equivalent to those described in Section 11 of this Policy. UK Users may lodge a complaint with the Information Commissioner's Office (ICO): https://ico.org.uk.

Data transfers to the USA take place on the basis of the UK-US Data Bridge (UK Extension to the EU-US Data Privacy Framework), as well as on the basis of Standard Contractual Clauses adapted for UK law (UK IDTA - International Data Transfer Agreement).

16.2. Switzerland (Federal Act on Data Protection - nFADP)

The provisions of the new Swiss Federal Act on Data Protection (nFADP, in force since 1 September 2023) apply to Users in Switzerland. Swiss Users may lodge a complaint with the Federal Data Protection and Information Commissioner (FDPIC): https://www.edoeb.admin.ch.

Data transfers to the USA take place on the basis of the Swiss-US Data Privacy Framework (Swiss-US DPF), as recognised by the FDPIC.

16.3. United States - California (CCPA / CPRA)

Residents of the State of California have additional rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), including:

- the right to know (right to know) what personal data are collected, used, disclosed, or sold
- the right to deletion of personal data
- the right to correction of inaccurate data
- the right to restrict the processing of sensitive personal data (Sensitive Personal Information - SPI)
- the right to opt out of the "sale" or "sharing" of personal data ("Do Not Sell or Share My Personal Information")
- the right to non-discrimination in connection with the exercise of the above rights

The Data Controller declares that it does not sell personal data within the meaning of the CCPA. Some forms of sharing data with advertising partners (Meta Pixel, Google Ads) may qualify as "sharing" under the CCPA. Users who do not wish their data to be shared for advertising purposes should withdraw consent to marketing cookies in the Website settings.

16.4. Canada (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to Users in Canada. Canadian Users have the right to access their data and to correct inaccuracies. The Data Controller appoints hi@muya.app as the contact point for the exercise of PIPEDA rights.

Complaints may be lodged with the Office of the Privacy Commissioner of Canada (OPC): https://www.priv.gc.ca.

16.5. Brazil (LGPD)

The Lei Geral de Proteção de Dados (LGPD, Law No. 13,709/2018) applies to Users in Brazil. Brazilian Users have the right of access, rectification, deletion, data portability, information on data sharing, and the right to withdraw consent. These rights may be exercised by contacting hi@muya.app.

The Data Controller has designated the contact address hi@muya.app as the contact point for the exercise of LGPD rights and as the point of contact with the Autoridade Nacional de Proteção de Dados (ANPD).

16.6. Japan (APPI) - Information for Future Users

The MUYA Application is not currently available in Japanese nor actively directed at the Japanese market. The provisions of the Act on the Protection of Personal Information (APPI) will be implemented before the Application is made available in the Japanese language version.

The Application is not currently targeting residents of Japan. Residents of Japan using the Application in a currently available language version do so voluntarily and accept the rules applicable under this Policy.

16.7. China (PIPL) - Information for Future Users

The Application is not currently officially available in a Chinese-language version nor dedicated to the Chinese market. Before making the Application available to residents of the People's Republic of China, the Data Controller will implement the requirements of the Personal Information Protection Law (PIPL), including in particular provisions concerning:

- mechanisms for data transfers outside the territory of China (CAC certification, Standard Contractual Clauses for China, or other approved mechanisms)
- rights of Users under PIPL (access, correction, deletion, withdrawal of consent, portability, and others)
- designation of a local representative in China, if required

The Application is not currently targeting residents of China. Residents of China using the Application in a currently available language version do so voluntarily and accept the rules applicable under this Policy.

17. Profiling and Automated Decision-Making

The Data Controller carries out profiling within the meaning of Art. 4(4) GDPR to a limited extent. Profiling consists of:

- analysis of audio playback history and favourite Content in order to generate personalised audio session suggestions in the Application
- segmentation of Newsletter subscribers in order to tailor the subject matter and frequency of dispatch (e.g. based on preferences indicated at sign-up)
- analysis of analytical events on the Website and in the Application (GA4, Firebase) for the purpose of optimising functionality and the relevance of marketing campaigns - solely on the basis of consent expressed in the cookie banner (Website) or in the consent prompt / Application settings (Application).

Profiling does not result in automated decisions being made with respect to the User within the meaning of Art. 22 GDPR - i.e. decisions producing legal effects or similarly significantly affecting the User. Personalised suggestions are of an auxiliary nature only.

The User has the right to object to profiling carried out on the basis of legitimate interests (Art. 6(1)(f) GDPR) by contacting the Data Controller at hi@muya.app.

18. Changes to the Privacy Policy

The Data Controller reserves the right to update this Policy in the event of:

- changes to legal provisions concerning personal data protection
- introduction of new Website or Application features
- changes to the list of sub-processors or the scope of processing
- other important reasons requiring an update to the Policy

Users will be informed of material changes to the Policy in advance - through a notice in the Application and/or by email to the address associated with the Account. The changes will enter into force no earlier than 14 days from the date of notification, unless they result from a legal obligation and require immediate implementation.

The current version of the Policy is always available on the Website www.muya.app and in the Application in the "Legal Information" section.

19. Contact

For all matters related to personal data protection, the exercise of Users' rights, and questions about this Privacy Policy, please contact:

- email: hi@muya.app
- correspondence address: Sopraya Sp. z o.o., ul. Krasińskiego 20, 64-800 Chodzież, Poland
- phone: +48 660 927 243

For complaints regarding the functioning of the Application and the Services provided, please contact: contact@sopraya.com.

- end of document -
Version 1.0 | Effective as of 15.05.2026