Privacy Policy

Overview: SyncLat LTD ("we" or "SyncLat") operates a platform connecting music industry stakeholders (producers, artists, supervisors) for music synchronization services. We are committed to protecting your privacy and handling personal data in compliance with the EU GDPR, UK GDPR, and related data protection laws. This Privacy Policy explains what data we collect, why and how we use it, with whom it is shared, how it is protected, and your rights as a data subject under GDPR. SyncLat is the data controller for the data we collect. If you have questions or concerns, you may contact our Data Protection Officer at **dpo@synclat.com**.

Data We Collect: We collect various categories of data from users on our platform:

- **Personal Identifiable Information (PII):** Name, email address, postal address, phone number, and other contact details provided when you register for an account or communicate with us. This also includes login credentials and profile information.
- **Music Content:** Audio files, stems, tracks and associated creative content uploaded by users (producers, artists) to share or license on the platform.
- **Payment and Financial Information:** Billing address, credit card or payment method details (handled via secure payment processors), transaction histories, and invoicing information needed to process payments for services or subscriptions. (We do not store full credit card numbers on our servers; payments are processed by trusted payment gateways.)
- **Metadata:** Information related to music licensing and usage such as track titles, ISRC codes, ownership and copyright details, license terms, and other metadata that describe the music content.
- **User Behavior Data:** Website and app usage data collected through cookies, analytics, and logging. This includes interaction logs, feature usage statistics, and aggregated tracking data (e.g., pages visited, clicks). We use tools like Google Analytics to understand platform usage. Cookies or identifiers used for analytics are considered personal data under GDPR 1 and are processed with appropriate

consent or legitimate interest.

Legal Bases for Processing: We rely on lawful bases under Article 6 GDPR for each category of processing:

- **Contractual Necessity:** Much of our processing is necessary to provide the platform services you requested. For example, we use your PII and music content to facilitate matches between producers and artists, to deliver content and features, and to process subscriptions or licensing agreements [2].
- **Consent:** We obtain your explicit consent for non-essential activities, such as sending marketing communications or using cookies/analytics, beyond strictly necessary ones [2]. You may withdraw consent at any time (it will be as easy to withdraw as to give consent [3]).

- **Legitimate Interests:** We may process certain data for legitimate business interests, such as improving our platform, securing our services, preventing fraud, and enforcing our policies [4] . Whenever we rely on legitimate interest, we ensure it does not override your rights and freedoms.
- **Legal Obligation:** We also process data to comply with legal and regulatory obligations (for example, accounting/tax requirements for payment records, financial reporting, or law enforcement requests).

Each processing purpose is documented and assessed under GDPR principles. Sensitive personal data (special categories) are not processed except as strictly required (e.g., metadata including personal opinions in lyrics would be treated as personal data only with explicit consent).

How We Use Data: We use the data for the following purposes (each aligned with a legal basis above):

- **Service Provision:** To match producers, artists, and supervisors as requested, and to enable communication and collaboration on music projects. This includes using PII to identify parties and facilitate contact, and using music content and metadata to manage licenses and rights.
- **Payments and Billing:** To process subscription fees, payments for licenses or services, and refunds. Payment data is shared only with PCI-compliant payment processors; we store only what is needed for invoices and auditing.
- **Platform Operation:** To maintain user accounts, authenticate users, and provide customer support. We use PII for account management and notify you about account changes or important updates.
- **Analytics and Improvement:** To analyze how users interact with the platform, diagnose technical issues, and improve features. We use Google Analytics and internal logs for aggregated site statistics. We only collect non-sensitive usage data, and any analytics cookies require consent [1] . IP addresses collected by analytics are anonymized whenever possible.
- **Communication:** To send you service-related notices (via email or in-app messaging) and, where consent is given, marketing newsletters about our services. You can opt out of marketing at any time.
- **Legal Compliance and Security:** To ensure compliance with laws (e.g., tax, accounting, GDPR), to detect and prevent fraud or abuse, and to enforce our Terms of Service. This includes monitoring for suspicious activity and sharing information with law enforcement if required by law.

Data Sharing and Third Parties: SyncLat may share data as follows:

- **Service Providers/Subprocessors:** We engage third-party vendors to help provide our services. These may include cloud hosting (e.g., AWS or equivalent), database management, payment processors (e.g., Stripe or PayPal), email or messaging services, analytics providers (e.g., Google Analytics) and other IT providers. Where possible, we use EU-based services or providers certified under adequate frameworks. All subprocessors have contracts requiring them to use the data only for SyncLat's purposes and to implement GDPR-level security. For example, AWS (EU regions) is EU-US Data Privacy Framework (DPF) certified 5 , and Google Analytics now operates under the EU-US DPF.
- **Other Users (where applicable):** Information you expressly share (e.g., published profile or samples) may be visible to other platform users as needed to facilitate collaboration (for example, a producer may see basic info about an artist they are negotiating with). We do not share your private contact details with other users without your consent.
- **Business Transfers:** In the event of a merger, sale, or acquisition, personal data may be transferred as part of the business assets, subject to confidentiality protections.

- **Legal Authorities:** We may disclose personal data if required to comply with a legal obligation (e.g., subpoena, court order) or to protect rights and safety (e.g., in cases of fraud or threats).

Generic categories of third-party services used (placeholders where specific names aren't given) include: cloud hosting providers, payment gateways, email/SMS delivery services, customer support platforms, AI/ ML service providers, and analytics/cookie tracking services.

International Data Transfers: SyncLat operates under the GDPR and UK GDPR and may transfer data outside the EU/EEA or UK in compliance with these laws. When data is sent to a country outside these regions (such as using AWS or Google services based in the U.S.), we rely on approved safeguards. Notably, AWS and Google are participants in the **EU-U.S. Data Privacy Framework (DPF)**, an adequacy mechanism adopted by the EU Commission on 10 July 2023 5 . The UK has likewise issued an adequacy decision for the DPF, allowing transfers to U.S. companies certified under the DPF without additional safeguards 6 . In cases where DPF does not apply, we implement **Standard Contractual Clauses (SCCs)** or other appropriate legal mechanisms for transfers. We do not rely on binding corporate rules. Data transfers are continuously monitored for compliance with updated data protection frameworks.

Data Retention: We retain personal data only as long as necessary for the purpose it was collected or as required by law. In alignment with the GDPR's storage limitation principle (personal data "must not be kept for longer than necessary" 7), we apply the following general retention periods:

- **PII (Account Information):** Retained while your account is active and for a reasonable period thereafter (e.g., up to 2 years of inactivity) to address any post-termination issues. If you delete your account or upon account closure, we will erase PII within 30 days, unless we require it longer to comply with legal obligations or resolve disputes.
- **Music Content and Metadata:** Kept for as long as required for any active licenses or projects you are involved in. After a license agreement ends or content is deleted by you, we will retain it for at most one year (unless you request earlier deletion) to allow for any legal claims.
- **Payment and Financial Records:** Stored in accordance with financial regulations (typically 7 years) for accounting and tax purposes. Only non-sensitive transactional details are kept (encrypted), and raw payment details are purged as soon as allowed by the payment processor.

- **Cookies and Analytics Data:** We use session cookies (deleted when you close your browser) and persistent cookies for logged-in sessions. Non-essential cookies (e.g., for Google Analytics) expire after user-level data is anonymized; Google Analytics 4, for example, allows up to 14 months of user-data retention [8] . We purge or anonymize analytics logs at least every 14 months.
- **System Logs and Access Records:** Security and audit logs (e.g., login attempts, admin actions) are retained for up to 12 months for security and compliance purposes. Less-sensitive operational logs may be kept for shorter periods (30–90 days) as needed for system troubleshooting [9] . We regularly review and purge outdated logs in accordance with our retention schedule.

We maintain a data retention policy and schedule specifying the exact durations for each data type [7] . Retention periods are periodically reviewed to ensure compliance with legal requirements and SyncLat's legitimate needs.

Data Subject Rights: Under the GDPR and UK GDPR, you have the following rights, which SyncLat facilitates:

- **Right to be Informed:** You can access this policy and receive clear information about how we process your data.
- **Right of Access:** You have the right to request confirmation of whether we process your personal data and to obtain a copy of that data 10 .
- **Right to Rectification:** You can request correction of inaccurate or incomplete personal data we hold about you 10 .
- **Right to Erasure ("Right to be Forgotten"):** You may ask us to delete your personal data when it is no longer needed for our purposes, or if you withdraw consent where consent was the only basis 10 . We will erase or anonymize data unless we have a compelling legal reason to retain it.
- **Right to Restrict Processing:** You can request the suspension of processing if you contest the accuracy of your data or object for some other reason while we verify your concerns 10 .
- **Right to Data Portability:** You have the right to receive your personal data (e.g., account profile) in a structured, commonly-used format and to transmit it to another controller, where applicable 10 .
- **Right to Object:** You may object to processing based on our legitimate interests or for direct marketing purposes, and we will cease that processing unless we demonstrate compelling legitimate grounds 10 .
- **Right to Withdraw Consent:** Where processing is based on consent (such as marketing emails or non-essential cookies), you can withdraw your consent at any time, and we will stop that processing. Withdrawals of consent do not affect processing done prior to withdrawal 11 .
- **Rights Related to Automated Decision-Making:** If we use any automated profiling or decision-making (e.g., AI recommendations), you have rights concerning the logic involved and the ability to request human intervention. (Currently, SyncLat does not perform automated decisions with legal effects on individuals, beyond personalized recommendations where you can always choose an alternative.)

You can exercise these rights by contacting **dpo@synclat.com** or using the in-app/privacy form. We will respond to requests within one month, as required by law 12 . If you are dissatisfied with our response, you have the right to lodge a complaint with your local data protection authority (e.g. the Information Commissioner's Ofice in the UK or your EU Member State's regulator).

AI-Generated Music: SyncLat may offer features that use AI to generate music from existing songs or mixes. Such features involve processing music content that may include personal data (e.g., an artist's voice or lyrics). When you use AI-generation tools, SyncLat will inform you and obtain your explicit consent to process your uploaded content for this purpose. We use appropriate safeguards (such as anonymization or pseudonymization where feasible) to minimize privacy risks. In line with recent EDPB guidance, we assess whether AI models trained on user data could inadvertently allow re-identification, and we take steps to reduce that risk 13 . You have the right to object to the use of your content in AI model training, and we will delete your content from the model if you request. We conduct Data Protection Impact Assessments (DPIAs) for high-risk processing activities like AI-assisted features 14 .

Logging and Monitoring: For security and accountability, we keep detailed logs of data processing activities. This includes records of user authentication (logins, password changes), administrative access, data exports/imports, modifications to user data, and key system events. Logs contain timestamps, user or admin identifiers, and the nature of the action (e.g., "user data viewed" or "file uploaded"). To protect log integrity, logs are stored in secure, access-controlled repositories (encrypted at rest and in transit) and are

write-once or regularly backed up to prevent tampering. We review security logs regularly for suspicious activity and have an incident response plan in case of breaches. Log retention is limited to the periods noted above (typically up to 1 year for security logs) 9 , after which old logs are securely deleted or anonymized.

Data Security: SyncLat implements appropriate technical and organizational measures to ensure data security and confidentiality. As required by GDPR Recital 83, we evaluate risks and implement measures like encryption where feasible 15 . All data in transit is encrypted via HTTPS/TLS. Sensitive personal data and payment information are stored encrypted at rest (e.g., using AES-256) 15 . Access to data is restricted on a need-to-know basis (principle of least privilege 16). We regularly test and update our security controls, train staff on data protection, and require subprocessors to meet equivalent security standards. In the event of a data breach involving personal data, we will notify affected users and authorities in accordance with GDPR notification timelines.

Cookies: We use cookies to enhance user experience and analyze site usage. Essential cookies (e.g., session cookies to keep you logged in) do not require consent, but we still inform users of their use. Non-essential cookies (e.g., analytics cookies) require your consent before use 1 . We use Google Analytics in compliance with its EU data protection guidelines, anonymizing IP addresses and respecting the retention settings described above. You may manage cookie preferences via our consent banner or your browser settings.

Accountability and Compliance: SyncLat maintains documentation of all its data processing activities (as per Article 30 GDPR) and reviews compliance regularly. We have appointed a Data Protection Oficer (DPO) who oversees GDPR compliance, contactable at **dpo@synclat.com**. Any changes to our Privacy Policy will be communicated via email or platform notices. Our goal is transparency and accountability in handling your data.

Sources: This policy and guide are informed by GDPR regulations and best practices 15 17 14 9 1 5 6 10 7 8 , among others. All references to GDPR or UK GDPR requirements are indicative of our commitment to legal compliance.

1 Cookies, the GDPR, and the ePrivacy Directive - GDPR.eu https://gdpr.eu/cookies/

2 4 Art. 6 GDPR – Lawfulness of processing - General Data Protection Regulation (GDPR) https://gdpr-info.eu/art-6-gdpr/

3 11 Rights of data subjects under GDPR https://nordlayer.com/learn/gdpr/data-subject-rights/

5 6 The EU-U.S. Data Privacy Framework - Amazon Web Services (AWS) https://aws.amazon.com/compliance/eu-us-data-privacy-framework/

7 Data retention and the GDPR: Best practices for compliance https://www.dpocentre.com/data-retention-and-the-gdpr-best-practices-for-compliance/

8 Data retention - Analytics Help https://support.google.com/analytics/answer/7667196?hl=en

9 21 GDPR Log Management: A Practical Guide for Engineers | Last9 https://last9.io/blog/gdpr-log-management/

10 GDPR Logging and Monitoring Best Practices | Mezmo https://www.mezmo.com/blog/best-practices-for-gdpr-logging

12 Respect individuals' rights | European Data Protection Board https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en

13 edpb.europa.eu https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

14 Data Protection Impact Assessment (DPIA) - GDPR.eu https://gdpr.eu/data-protection-impact-ass

essment-template/

15 Recital 83 - Security of Processing - General Data Protection Regulation (GDPR) https://gdpr-info.eu/recitals/no-83/

16 18 19 20 Protect Data Everywhere - OWASP Developer Guide https://devguide.owasp.org/en/04-design/02-web-app-checklist/08-protect-data/

17 Art. 25 GDPR – Data protection by design and by default - General Data Protection Regulation (GDPR) https://gdpr-info.eu/art-25-gdpr/

Privacy Policy edited and simplified (07-06-2025)

Overview

SyncLat LTD (“we” or “SyncLat”) operates a platform that connects music industry stakeholders—including producers, artists, and supervisors—for music synchronization services. We are committed to protecting your privacy and handling your data in accordance with the EU General Data Protection Regulation (GDPR), UK GDPR, and other applicable data protection laws.

This Privacy Policy outlines what personal data we collect, why and how we use it, with whom it may be shared, how it is protected, and your rights as a data subject under applicable law. SyncLat acts as the data controller for personal data we collect. If you have questions, please contact our Data Protection Officer at dpo@synclat.com**.**

Data We Collect

We collect the following categories of data from users of our platform:

- Personally Identifiable Information (PII): Name, email address, phone number, postal address, and other contact details provided during registration or communication. This includes profile data and login credentials.

- Music Content: Audio files, stems, tracks, and other creative materials uploaded by users to share or license via the platform.

- Payment and Financial Information: Billing addresses, payment method details (processed securely via third-party providers), and transaction history. We do not store full card details on our servers.

- Metadata (Retained and Processed): We collect and retain music-related metadata such as track titles, ISRC codes, ownership and rights information, licensing terms, and descriptive attributes about uploaded content. Metadata is essential to our platform's operation and is preserved for ongoing licensing, usage tracking, dispute resolution, and music discovery.

- User Behavior Data: Website and app interaction data such as feature usage, pages visited, and clicks. This includes data collected through cookies and analytics (e.g., Google Analytics), which may be classified as personal data under the GDPR.

Legal Bases for Processing

We process your personal data under the following lawful bases, as defined in Article 6 of the GDPR:

- Contractual Necessity: Most data we collect is required to deliver the services you request. This includes your PII, music content, and metadata to enable platform functionality, content sharing, and communication between users.

- Consent: We request your explicit consent for optional activities like marketing emails and non-essential cookies or analytics. You may withdraw your consent at any time.

- Legitimate Interests: We retain and use metadata and behavioral data to ensure platform functionality, track content usage, maintain music rights information, and improve our services. We always balance these interests against your fundamental rights and freedoms.

- Legal Obligation: We retain certain data to comply with tax, financial reporting, and legal regulations.

We do not process special categories of personal data unless explicitly consented or required for a legal purpose.

How We Use Data

We use your data for the following purposes:

- Service Delivery: To match and connect music professionals, enable

communication, and manage licensing agreements. Metadata is essential for cataloging music, enforcing rights, and supporting discovery.

- Payments: To process billing, license fees, and subscriptions securely using PCI-compliant third parties.

- Platform Operation: To maintain and support accounts, authenticate users, and enable features.

- Analytics and Platform Improvement: To understand user behavior, improve features, and monitor usage through tools like Google Analytics. We process only non-sensitive, aggregated data with your consent.

- Communication: To send service-related messages and, where permitted, marketing content. You may opt out of marketing communications at any time.

- Compliance and Security: To enforce our terms, prevent abuse, and fulfill regulatory requirements. This includes analyzing metadata and user behavior to detect misuse.

Data Sharing and Third Parties

We may share data with:

- Service Providers: Third-party vendors such as cloud hosts (e.g., AWS), analytics services (e.g., Google), email/messaging providers, and payment processors (e.g., Stripe). All vendors are contractually bound to use the data only for SyncLat's purposes and meet strict security and privacy standards.

- Other Users: Public profiles and shared content may include metadata visible to other users (e.g., track title, license status). Private contact information is never shared without your consent.

- Legal Authorities: Data may be shared if required by law or in response to valid legal requests.

- Business Transfers: In case of a sale, merger, or acquisition, personal data (including metadata) may be part of the transferred assets, subject to privacy safeguards.

International Data Transfers

If data is transferred outside the EU or UK (e.g., to the US via AWS or Google services), we rely on legal mechanisms like the EU-U.S. Data Privacy Framework or Standard Contractual Clauses. We monitor all data transfers for compliance and maintain updated assessments to ensure your data is protected regardless of location.

Data Retention

We retain data only as long as necessary:

- PII and Account Data: Retained for the duration of your account and up to 2 years after inactivity. If you request deletion, we erase PII within 30 days unless legal obligations apply.
- Metadata: Retained indefinitely where necessary for licensing, dispute resolution, service operation, platform analytics, and rights verification. Metadata is integral to music industry standards and enables our users to manage and track content over time.
- Music Content: Retained for the duration of active licenses or projects, and deleted within 12 months after completion or user deletion request.
- Payment Records: Retained for up to 7 years for legal and tax compliance.
- Analytics and Logs: Session cookies are cleared when browsers close; analytics data is retained for up to 14 months. Logs for security and compliance are stored for up to 12 months.

We review and securely delete or anonymize expired data in line with GDPR principles.

Data Subject Rights

As a data subject, you have the following rights:

- Access, correction, or deletion of your data
- Restriction or objection to processing (including metadata)
- Portability of your data to another service
- Withdrawal of consent at any time
- Right to lodge a complaint with your local data protection authority

To exercise your rights, contact dpo@synclat.com or use the in-app privacy tools. We will respond within 30 days as required by law.

AI-Generated Music and Metadata

Some SyncLat features may include AI tools that generate music using your uploaded content. These tools may process metadata (e.g., genre, mood, voice data) to produce outputs. We inform users and request explicit consent before using content in AI systems. You may opt out and request deletion of your data from these systems at any time. We apply anonymization techniques and conduct regular risk assessments to mitigate re-identification or misuse of metadata.

Logging and Monitoring

We maintain detailed logs of platform activity, including metadata processing, to ensure system integrity and accountability. Logs are encrypted, access-controlled, and reviewed regularly. Security logs are retained for up to 12 months and then securely purged or anonymized.

Data Security

We protect your data using industry-standard security measures, including encryption (TLS in transit, AES-256 at rest), access controls, and secure backups. All metadata and music content are handled with equal protection as personal data. Our team is trained on data privacy best practices, and subprocessors are required to meet equivalent security standards.

Cookies

We use essential cookies for platform functionality and non-essential cookies for analytics and marketing, subject to your consent. You can manage cookie preferences via the cookie banner or your browser settings.

Accountability

We maintain a record of our processing activities (per Article 30 GDPR), and review

compliance regularly. Our DPO monitors adherence to privacy obligations. We notify users of any changes to this Privacy Policy via email or in-app notice.

Contact

Data Protection Officer
Email: dpo@synclat.com