DATA PRIVACY POLICY

LAST UPDATED **MARCH 6, 2026**

TOPICS

This Data Privacy Policy for Lyriem ("we," "us," or "our") is a supplementary policy to our Privacy Policy and Terms and Conditions. It describes in detail how we collect, anonymize, use, and sell data generated through our platform, and the rights and controls available to you regarding that data. Lyriem is a freelancer marketplace connecting clients and independent contractors. Our platform handles job postings, contracts, milestone payments via Stripe, reviews, and reputation data. As part of our business model, we generate anonymized datasets from aggregated platform activity and sell these datasets to third-party buyers for workforce analytics, AI model training, and market intelligence. This policy exists to provide full transparency into how your data flows through our platform, what happens to it before it is sold, what protections are in place, and what choices you have. We believe you deserve to understand exactly what is happening with your data — not buried in legal boilerplate, but stated plainly. If you have questions about this policy, contact us at austin.riggs@lyriem.com.

OUR DATA MODEL 3.01

In Short: Lyriem operates a dual data model: we use your personal data to run the platform, and we sell anonymized platform activity data to third parties. Lyriem's data model has two distinct layers:

Layer 1: Personal data for platform operations
We collect and use your personal information — such as your name, email address, payment details, and professional profile — to operate the platform, facilitate transactions between clients and freelancers, process payments, and provide customer support. This data is used solely for delivering and improving the Services and is governed by our Privacy Policy.

Layer 2: Anonymized data for commercial sale
We generate anonymized, aggregated datasets from platform activity and sell them to third-party buyers. Before any data leaves our platform for commercial sale, all personally identifiable information is removed or replaced with synthetic identifiers. The resulting datasets contain patterns, trends, and analytics — not individual user profiles.

These two layers are distinct. Your identifiable personal data is never sold to third parties unless you have explicitly opted in to allow it (see Section 3.07). The anonymized datasets sold to buyers cannot be used to identify individual users.

WHAT DATA WE COLLECT 3.02

In Short: We collect personal information you provide, transaction data generated through platform use, and technical data collected automatically.

Personal information you provide
This includes data you provide when creating an account or using the Services:

- Full name
- Email address
- Phone number
- Mailing and billing addresses

- Job title and professional qualifications
- Username and password
- Social Security number (where required for tax or payment compliance)
- Payment instrument details (handled and stored by Stripe)
- Social media profile data (if you register via social login)
- Portfolio, work history, and skills information

Platform activity data
This includes data generated through your use of the Services:

- Project postings, proposals, and contract details
- Transaction values, milestone payments, and payment history
- Review and rating content and scores
- Messaging frequency and response times (not message content)
- Skills, categories, and service types associated with projects
- Project completion rates and delivery timelines
- Dispute and resolution data

Technical and device data
This includes data collected automatically when you use the Services:

- IP address and approximate geographic location
- Browser type, version, and settings
- Device type, operating system, and language preferences
- Referring URLs and pages visited within the Services
- Log and usage data, including timestamps and session duration

HOW WE CAN ANONYMIZE YOUR DATA 3.03

In Short: We fully mask or replace all personally identifiable information with synthetic data before any dataset is sold. Anonymization is the process by which we remove or replace all information that could identify an individual user. We employ two methods:

Method 1: Complete masking
Personal identifiers are fully stripped from the dataset. Fields such as name, email, phone number, address, Social Security number, and payment details are entirely removed, leaving only non-identifiable platform activity data.

Method 2: Synthetic replacement
Real personal data is replaced with fabricated, synthetic identifiers that bear no relationship to actual users. For example, a user's real name may be replaced with a randomly generated name, and their email with a synthetic email address. This allows datasets to retain structural integrity for analytics purposes without exposing any real user information. When anonymization occurs Anonymization is performed on demand, immediately before any dataset is prepared for sale to a third-party buyer. Your live, identifiable data stored in our platform databases is never directly transferred to buyers. Each dataset undergoes a fresh anonymization process at the point of preparation.

What gets anonymized
The following categories of personally identifiable information are always anonymized before any data sale:

DATA CATEGORY	EXAMPLES	ANONYMIZATION METHOD
Identity	Name, username, profile photo	Fully masked or synthetic replacement
Contact	Email, phone number, mailing address	Fully masked or synthetic replacement
Financial Identity	SSN, payment card numbers, billing address	Fully masked (never synthetically replaced)
Authentication	Passwords, security questions, login tokens	Fully masked (never included in any dataset)
Social Media	Linked social profiles, friends lists	Fully masked
Device Identifiers	IP address, device ID, browser fingerprint	Fully masked or generalized (e.g., region-level only)

Re-identification safeguards
We implement safeguards to minimize the risk of re-identification from anonymized datasets:

- Aggregation thresholds: Data points are only included in datasets when they represent a sufficient volume of users, preventing individual activity from being isolated.
- Cross-referencing controls: Contractual and technical controls prohibit buyers from attempting to re-identify users by combining our datasets with external data sources.
- Ongoing review: We periodically review our anonymization methods to ensure they remain effective against evolving re-identification techniques.

WHAT ANONYMIZED DATASETS CONTAIN 3.04

In Short: Anonymized datasets contain platform activity patterns, trends, and analytics — not individual user profiles. Once anonymized, the datasets we sell may contain the following types of non-identifiable platform activity data:

- Transaction volume and value patterns (without identifying parties to any transaction)
- Project categories, subcategories, and completion rates
- Skill demand and supply trends across the platform
- Pricing and hourly rate benchmarks by category, skill, and region
- Geographic demand patterns (aggregated to city or region level, not individual addresses)
- Average response times and engagement metrics
- Contract milestone structures and delivery timelines
- Review and rating distributions by category
- Freelancer availability and capacity trends
- Industry and vertical hiring patterns
- Seasonal and time-based demand fluctuations

These datasets do not contain names, email addresses, phone numbers, payment details, or any other information that could identify a specific user.

WHO WE SELL DATA TO AND HOW IT MAY BE USED 3.05

In Short: We sell anonymized data to enterprise buyers for workforce analytics, AI training, and market intelligence.

Categories of buyers
We sell anonymized datasets to the following categories of third-party buyers:

- Enterprise HR departments — for workforce planning, compensation benchmarking, and talent strategy
- Workforce analytics and consulting firms — for market research, labor market analysis, and advisory services
- Staffing and recruitment agencies — for demand forecasting, rate benchmarking, and talent pool analysis
- Research institutions — for academic and applied research on labor markets and the gig economy

How buyers may use the data
Anonymized datasets may be used by buyers for:

- API feeds: Integration into workforce analytics platforms and internal dashboards
- AI and machine learning models: Training predictive models for talent demand, pricing, and workforce optimization
- Data packages and reports: Packaged market intelligence products, benchmarking reports, and industry analyses
- Strategic planning: Internal workforce planning, budgeting, and resource allocation decisions

Buyers are not permitted to use the data to identify, contact, or target individual Lyriem users.

CONTRACTUAL RESTRICTIONS ON DATA BUYERS 3.06

In Short: All buyers are bound by strict contractual obligations that prohibit re-identification and unauthorized redistribution. Every third-party data buyer enters into a Data Purchase Agreement with Lyriem that includes the following binding restrictions:

Prohibition on re-identification
Buyers are strictly prohibited from attempting to re-identify any individual user from the anonymized datasets, including by cross-referencing with other data sources, public records, social media, or any other information. Any attempt at re-identification constitutes a material breach of the agreement.

No unauthorized resale or redistribution
Buyers may not resell, sublicense, redistribute, or transfer any Lyriem data to any third party without our explicit written approval. Approved redistribution is subject to the same contractual restrictions that apply to the original buyer.

Security requirements
Buyers must implement reasonable technical and organizational security measures to protect the datasets from unauthorized access, disclosure, alteration, or destruction.

Permitted use limitations
Buyers may only use the data for the purposes specified in their Data Purchase Agreement. Use of the data forpurposes not approved by Lyriem is prohibited.

Audit rights
Lyriem reserves the right to audit buyer compliance with the terms of the Data Purchase Agreement, including the re-identification prohibition and security requirements.

Breach consequences
Violation of any restriction in the Data Purchase Agreement will result in immediate termination of the agreement, revocation of access to all datasets, and may result in legal action including claims for damages.

OPT-IN SALE OF NON-ANONYMIZED PERSONAL DATA 3.07

In Short: Users may voluntarily opt in to allow the sale of their real personal data. This is entirely optional and does not affect platform access. Lyriem offers users the option to opt in to the sale of their non-anonymized personal data to third-party buyers. This means that, if you choose to opt in, your real name, professional profile, skills, work history, and contact information may be included in datasets sold to buyers.

How opt-in works

- Opt-in is managed through your account privacy dashboard under "Data Sale Preferences."
- Opt-in is entirely voluntary. You are never required to opt in to use the platform.
- You can opt out at any time through the same dashboard. Once you opt out, your non-anonymized personal data will not be included in any future data sales.
- Opting out does not affect your ability to use the Services or the quality of service you receive. You will not be discriminated against for exercising your rights.

What opt-in covers
If you opt in, the following personal data may be included in sold datasets in non-anonymized form:

- Full name and professional title
- Professional profile, including skills, certifications, and work history
- Contact information (email, phone number)
- Review and rating history associated with your real profile

Opt-in never covers sensitive personal information such as Social Security numbers, payment card details, or authentication credentials. These are never sold in any form.
What opt-in does not affect
Regardless of your opt-in or opt-out status, your platform activity data (transaction patterns, project types, skills demand data, engagement metrics, etc.) will always be included in anonymized, aggregated datasets that are sold to third parties. This anonymized data cannot be used to identify you. The opt-in choice applies only to whether your real personal identifiers are attached to the data.

YOUR RIGHTS AND CONTROLS 3.08

In Short: You have the right to access, correct, delete, and control the sale of your personal data through your account privacy dashboard.

Privacy dashboard
Your account includes a privacy dashboard where you can:

- View what personal data we hold about you
- Manage your opt-in/opt-out preference for non-anonymized data sale
- Submit a request to access, correct, or delete your personal data
- Download a copy of your personal data (data portability)
- Withdraw consent for specific processing activities

Core rights available to all users
Regardless of where you are located, we provide the following rights to all Lyriem users:

- Right to know: You can request a clear explanation of what personal data we collect, how it is used, and who it is shared with or sold to.
- Right to access: You can request a copy of the personal data we hold about you.
- Right to correction: You can request that we correct inaccurate or incomplete personal data.
- Right to deletion: You can request that we delete your personal data from our active databases, subject to legal retention requirements.
- Right to opt out of data sale: You can opt out of the sale of your non-anonymized personal data at any time.
- Right to non-discrimination: You will not be penalized, charged differently, or provided a different level of service for exercising any of your data rights.

How to exercise your rights
You can exercise your rights through any of the following methods:

- Privacy dashboard: Log in to your account and navigate to privacy settings.
- Email: Send a request to **austin.riggs@lyriem.com** with the subject line "Data Rights Request."
- Mail: Write to Lyriem, PO BOX.

We will acknowledge your request within 10 business days and fulfill verified requests within 45 days as required by applicable law. If additional time is needed, we will notify you of the reason and the extended timeline.

CCPA AND US STATE PRIVACY COMPLIANCE 3.09

In Short: We comply with the California Consumer Privacy Act (CCPA) and similar US state data protection laws. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), grants California residents specific rights regarding their personal information. Similar laws exist in Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia. We extend the following rights to residents of all these states.

Definition of 'sale' under CCPA
The CCPA defines "sale" broadly as the transfer of personal information for monetary or other valuable consideration. Under this definition, the following Lyriem activities may constitute a "sale":

- The sale of anonymized datasets derived from platform activity to third-party buyers (although the CCPA generally exempts truly de-identified data, we disclose this activity for full transparency)
- The sale of non-anonymized personal data for users who have opted in under Section 7 of this policy

"Do Not Sell or Share My Personal Information"
In compliance with CCPA, we provide the following mechanisms to opt out of the sale of your personal information:

- Privacy Dashboard: Log in to your account and navigate to your data sale preferences.
- Email: Submit a request to austin.riggs@lyriem.com with the subject line "Do Not Sell My Personal Information."
- Authorized agent: You may designate an authorized agent to submit an opt-out request on your behalf. We may require proof of authorization.

Categories of personal information sold or shared
In the preceding twelve (12) months, we have sold or shared the following categories of personal information to third parties:

CATEGORY	SOLD/SHARED	FORM	RECIPIENTS
Identifiers (name, email, etc.)	Only with user opt-in	Non-anonymized	HR depts, workforce firms, staffing agencies
Personal Information (CA Customer Records)	Yes	Anonymized	HR depts, workforce firms, staffing agencies, research institutions
Commercial information	Yes	Anonymized	Same as above
Internet/ network activity	Yes	Anonymized	Same as above
Professional Information	Yes	Anonymized	Same as above
Inferences	Yes	Anonymized	Same as above
Sensitive personal information	Never sold	N/A	N/A

Request verification and appeals
Upon receiving your request, we will verify your identity before processing. If we cannot verify your identity from existing information, we may request additional verification. If we decline your request, you may appeal by emailing **austin.riggs@lyriem.com**. If your appeal is denied, you may file a complaint with your state attorney general. California "Shine The Light" law California Civil Code Section 1798.83 permits California residents to request information about personal data disclosed to third parties for direct marketing purposes once per year, free of charge. To make such a request, contact us at **austin.riggs@lyriem.com**.

GDPR COMPLIANCE 3.10

In Short: While we currently store and process all data in the United States, we recognize the rights established by the General Data Protection Regulation (GDPR) and provide information for users located in the EEA, UK, or Switzerland.

Legal basis for processing
Where GDPR applies, we process personal data under the following legal bases:

- Contract performance: Processing necessary to provide the Services you have requested (account management, payments, communications).
- Explicit consent: Processing of personal data for sale to third parties in non-anonymized form (opt-in only, per Section 7).
- Legitimate interest: Processing for security, fraud prevention, platform improvement, and generation of anonymized datasets for commercial sale, where such processing does not override your fundamental rights and freedoms.
- Legal obligation: Processing required to comply with applicable laws, tax requirements, and legal processes.

GDPR rights
If you are located in the European Economic Area (EEA), the United Kingdom, or Switzerland, you have the following rights under the GDPR in addition to the rights listed in Section 8:

- Right to data portability: You can request your personal data in a structured, commonly used, machine-readable format.
- Right to restriction of processing: You can request that we restrict processing of your personal data in certain circumstances.
- Right to object: You can object to processing based on legitimate interest, including the generation of anonymized datasets from your activity data.
- Right not to be subject to automated decision-making: You have the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal effects or similarly significant effects concerning you.

International data transfers
All personal information is stored and processed exclusively in the United States on Amazon Web Services (AWS) infrastructure. We do not currently operate under the EU-US Data Privacy Framework or maintain Standard Contractual Clauses (SCCs). If you are located in the EEA, UK, or Switzerland and have concerns about cross-border data transfers, please contact us at austin.riggs@lyriem.com before using the Services.

Data Protection Officer
We intend to appoint a Data Protection Officer (DPO) in the future. Until a DPO is appointed, all data protection inquiries should be directed to **austin.riggs@lyriem.com**.

DATA RETENTION AND DELETION 3.11

In Short: Identifiable personal data is retained while your account is active. Anonymized datasets are retained indefinitely.

Personal data retention
We retain your identifiable personal data for as long as your account remains active on the platform. When you delete your account or request deletion of your data, we will remove your personal information from our active databases, subject to the following exceptions:

- Legal retention: We may retain certain data as required by tax, accounting, or other legal obligations.
- Fraud prevention: We may retain limited data necessary to prevent fraud, enforce our terms, or assist with investigations.
- Backup archives: If personal data exists in backup archives, it will be securely isolated and deleted when the backup cycle completes.

Anonymized data retention
Anonymized and aggregated datasets are retained indefinitely. Because these datasets do not contain personally identifiable information, they do not constitute personal data and are not subject to deletion requests.

What happens to your data after account deletion
Upon account deletion:

- Your identifiable personal data will be removed from our active databases within 30 days.
- Any data that has already been anonymized and sold to third parties prior to your deletion request cannot be recalled or removed from those third-party datasets, as the data no longer contains identifiers linking it to you.
- Any data that has not yet been anonymized and sold will not be included in future datasets after your deletion request is processed.
- If you previously opted in to non-anonymized data sale, any personal data already sold cannot be recalled. However, your personal data will not be included in any future non-anonymized sales after your deletion request.

DATA SECURITY 3.12

In Short: We implement encryption and AWS security infrastructure to protect your data. We have implemented the following technical and organizational security measures:

- Encryption in transit: All data transmitted between your device and our servers is encrypted using TLS (Transport Layer Security).
- Encryption at rest: Personal data stored in our databases is encrypted at rest using AES-256 encryption via AWS.
- Infrastructure security: Our platform is hosted on Amazon Web Services (AWS), which provides network firewalls, DDoS mitigation, and physical security controls.
- Access controls: Access to personal data is restricted to authorized personnel on a need-to-know basis.
- Anonymization pipeline security: The anonymization process occurs in a controlled environment with access restricted to authorized data operations personnel.

Despite these measures, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure. We cannot promise that unauthorized third parties will not be able to defeat our security measures. Transmission of personal information to and from our Services is at your own risk.

THIRD-PARTY SERVICE PROVIDERS 3.13

In Short: We share personal data with Stripe for payments and use AWS for hosting. These providers do not receive data through our commercial data sale program. Separately from our anonymized data sales, we share personal information with the following service providers who perform services on our behalf:

Stripe
Purpose: Payment processing. Stripe handles and stores all payment data, including credit/debit card numbers and billing information. Stripe processes payments as an independent data controller. Privacy notice: https://stripe.com/privacy

Amazon Web Services (AWS)
Purpose: Cloud hosting and data storage infrastructure. All Lyriem data, including personal information and anonymized datasets, is stored on AWS servers located in the United States. AWS processes data as a data processor on our behalf. Privacy notice: https://aws.amazon.com/privacy/

Government and legal requests
We may disclose your personal information to United States government entities solely in response to valid legal requests, including subpoenas, court orders, or other legal processes required by law. We do not proactively share user data with government agencies.

Business transfers
In the event of a merger, acquisition, financing, or sale of all or a portion of our business, your personal information and our anonymized datasets may be transferred to the acquiring entity. We will notify you of any such transfer and any changes to this policy that result from it.

DATA BREACH NOTIFICATION 3.14

In Short: We will notify affected users and relevant authorities in the event of a data breach. In the event of a data breach that compromises the security of your personal information, we will:

- Investigate the breach promptly and take steps to contain and remediate it.
- Notify affected users without unreasonable delay via email and/or prominent notice on the Services.
- Notify relevant regulatory authorities as required by applicable law, including within 72 hours where required by GDPR.
- Provide you with information about the nature of the breach, the categories of data affected, and the steps we are taking to address it.

We are actively developing a formal incident response plan to ensure timely and structured breach notification. If you believe your data has been compromised, contact us immediately at **austin.riggs@lyriem.com**.

CHILDREN'S DATA 3.15

In Short: We do not knowingly collect or sell data from anyone under 18. Lyriem is intended for users who are at least 18 years old. We do not knowingly collect, solicit data from, or market to children under 18 years of age. We never knowingly sell personal information of users under 18. If we learn that we have collected personal information from a user under 18, we will deactivate the account and take reasonable measures to promptly delete the data from our records and ensure it is excluded from any anonymized datasets not yet sold. If you become aware of any data we may have collected from a minor, please contact us at **austin.riggs@lyriem.com**.

CHANGES TO THIS POLICY 3.16

In Short: We will notify you of material changes, especially changes to our data sale practices. We may update this Data Privacy Policy from time to time. The updated version will be indicated by an updated "Last updated" date at the top of this document.
If we make material changes to this policy — particularly changes to our anonymization methods, the categories of data sold, the types of buyers we sell to, or the rights and controls available to you — we will notify you by:

- Prominently posting a notice on the Services
- Sending you a direct notification via email
- Requiring re-acknowledgment of the updated policy where appropriate

We encourage you to review this policy periodically. Your continued use of the Services after any changes constitutes your acceptance of the updated policy.

CONTACT US 3.17

If you have any further questions or comments or wish to report any problematic Content or Contribution, you may contact us by: **Email: austin.riggs@lyriem.com**