The Pending Agency
Privacy Policy
Last Updated: April 2026

1. Data Controller

The entity responsible for processing your personal data under Article 4(7) GDPR is:

The Pending GmbH

Arthur-Müller-Straße 24, 12487 Berlin, Germany

Charlottenburg HR-Nr.: HRB250720B | USt.-ID: DE360039760 | Steuer-Nr.: 37/557/52192

Managing Director: Tim Kriegler

Email: info@thepending.app | service@thepending.app

2. Data Protection Contact

For all data protection enquiries, please contact us at service@thepending.app or at the postal address above. Please mark correspondence "Privacy / Data Protection".

Note: The Pending GmbH is not currently required to appoint a formal Data Protection Officer under Article 37 GDPR. If this changes as the Platform scales, we will update this policy accordingly.

3. About The Pending Agency

The Pending Agency is a SaaS platform connecting managers, bookers, and casting professionals with artists and creatives. Managers can post projects and casting calls, discover artists via AI-powered search, and manage applications. Artists maintain portfolios, apply to opportunities, and use AI-assisted career tools. The Platform is operated by The Pending GmbH and hosted on Amazon Web Services (AWS) infrastructure in the EU (eu-central-1, Frankfurt).

4. Categories of Data Subjects

We process personal data about the following categories of individuals:

- Managers — Companies and individuals who post projects and search for artists.
- Artists — Individuals with portfolios who apply to opportunities on the Platform.
- Applicants (non-registered) — People who apply to jobs or casting calls without a Platform account (e.g., via email). Their data is stored as submitted by the applicant and processed on behalf of the manager posting the opportunity.
- Manual Profile Subjects — Third parties whose profiles are created by managers (e.g., scouted artists not yet registered). Managers are responsible as Data Controller for this data.
- Website Visitors — Anonymous users browsing public pages.
- CRM Contacts — Business contacts added by artists via the Pocket CRM feature.

5. Personal Data We Collect and Why

5.1 Account and Identity Data

When you register, we collect your name, email address, and (if applicable) payment details. We process this data to create and manage your account and deliver the Service. Legal basis: Article 6(1)(b) GDPR (performance of a contract).

5.2 Artist Portfolio and Profile Data

Artists provide professional information including name, location, skills, bio, portfolio links, contact details, and profile pictures. This data powers the Platform's discovery and application features. Legal basis: Article 6(1)(b) GDPR.

Artists may optionally provide special category data (e.g., gender identity, citizenship, physical characteristics, languages) via the personal details section of their profile. You are never required to provide this information to use the Platform. The legal basis depends on your visibility settings: where you choose to make this data publicly visible on your profile, processing is based on Article 9(2)(e) GDPR (data manifestly made public by the data subject). Where you restrict visibility to registered users only, processing is based on your consent (Article 9(2)(a) GDPR), expressed through the act of knowingly entering and saving this data with restricted visibility. You may withdraw consent at any time by removing the data from your profile.

5.3 Application and Project Data

If you post or apply to job openings or casting calls, we store the content of those postings and applications, including any form responses, attachments, and correspondence. Managers who post opportunities are Data Controllers for the personal data of their applicants (see Section 9). Legal basis: Article 6(1)(b) GDPR.

5.4 Spotty and AI Interaction Data

When you interact with Spotty (via in-app chat or email), your inputs, the actions taken, and the AI responses are logged to provide the service and for quality and safety review. These logs may include excerpts of profile data or application content that Spotty references. Legal basis: Article 6(1)(b) GDPR. We do not use your Spotty interactions to train AI models.

5.5 Roster, Manual Profiles, and CRM Contacts

Managers may create manual profile entries for artists not registered on the Platform, and artists may add contacts to the Pocket CRM. The person entering this data is the Data Controller for it. The Pending GmbH processes it as a Data Processor on their behalf. Legal basis for our processing: Article 6(1)(b) GDPR (performance of contract with the user entering the data); the user entering the data must separately ensure they have a lawful basis for holding this information.

5.6 Automatically Collected Technical Data

We automatically collect IP addresses, device and browser information, access logs, and usage patterns for security, performance, and troubleshooting purposes. Login attempts are logged for fraud prevention. Legal basis: Article 6(1)(f) GDPR (legitimate interest in platform security and stability).

5.7 Billing and Financial Data

Subscription and payment processing is handled by Stripe. We store only a Stripe customer ID and subscription ID. No payment card details are stored on our servers. Legal basis: Article 6(1)(b) GDPR.

5.8 Social Login Data

If you register or log in via Google, Apple, or Microsoft, we receive your name, email, and (where provided) profile picture from that provider. Legal basis: Article 6(1)(a) GDPR (consent, expressed via your choice of login method).

5.9 OAuth and Cloud Document Tokens

If you connect a cloud storage service (Google Drive, Microsoft OneDrive, Notion), we store the OAuth tokens required to access your files on your behalf. These are stored securely and used only for the features you activate. Legal basis: Article 6(1)(b) GDPR.

6. How We Use AI

The Platform uses AI across several features:

- Spotty (Manager) — Conversational AI assistant that performs project management tasks on your behalf.
- Spotty (Artist) — Conversational AI assistant for opportunity discovery, application drafting, and career management.
- Talent Finder — AI-powered talent discovery that processes your search queries and publicly available profile data to suggest artists.
- Application Analysis — AI scoring and evaluation of incoming applications to help managers review candidates. Scores are displayed to managers as decision-support tools, not binding assessments.
- Profile Analysis — AI analysis of portfolio profiles to power search rankings and recommendations.
- Embeddings — Semantic vector representations of profile text used to power similarity search.
- Email Classification — Categorizes inbound emails (application, inquiry, spam) for inbox management.
- Job Finder — AI-powered matching of jobs and casting calls to artist profiles, based on skills, location, and portfolio content.
- Application Assistant — AI tool that generates form responses and cover letters based on artist portfolio data and the job requirements.
- Client Finder — AI-powered discovery of potential clients for artists, part of the Pocket CRM feature, based on portfolio data and industry context.

All AI features use models accessed via AWS Bedrock (eu-central-1), including Claude by Anthropic and Amazon Titan. AWS Bedrock does not use your data to train AI models.

Where AI features influence the visibility or ranking of artist profiles or applications (e.g., search rankings, application scores), this constitutes automated processing that may affect you. You have the right to request human review of any AI-generated outcome, to express your point of view, and to contest the result. Contact service@thepending.app to exercise this right.

7. Third-Party Service Providers

We share personal data with the following categories of third-party processors, each subject to a Data Processing Agreement:

- Infrastructure (AWS, Frankfurt) — Hosting, database, file storage, email sending and receiving, AI model inference.
- Payment (Stripe) — Subscription billing and payment processing. Stripe is certified PCI-DSS compliant.
- AI and Search (AWS Bedrock, Tavily, Jina AI, Firecrawl) — AI model inference and web search for AI features. Search queries derived from user input may be sent to third-party search services (US-based). We are in the process of obtaining Data Processing Agreements with all relevant providers. Where DPAs are not yet finalized, we minimize data sent to these services to non-personal query strings where technically possible.
- Translation (DeepL, Germany) — Dynamic content translation. DeepL is EU-based.
- Social Login (Google, Apple, Microsoft) — Authentication data from third-party login providers. Data transferred to the US under Standard Contractual Clauses.

- Cloud Document Integrations (Google Drive, Microsoft OneDrive/SharePoint, Notion) — File access for users who opt to connect these services. Data transferred under Standard Contractual Clauses.
- Bot Protection (Cloudflare Turnstile) — Anti-bot verification on login and signup. IP address and browser signals processed.
- Geocoding (OpenCage, Germany) — Location text (city/country) converted to geographic coordinates for portfolio features.
- Analytics (Google Analytics 4, planned) — Aggregated usage analytics, activated only after cookie consent.

8. International Data Transfers

The Platform is hosted in AWS eu-central-1 (Frankfurt, Germany). Some of our third-party processors are based in the United States or other countries outside the EU/EEA. For all such transfers, we rely on Standard Contractual Clauses (2021 version) approved by the European Commission, supplemented by Transfer Impact Assessments where required.

9. Cookies and Tracking

We use the following cookies:

- sessionid — Keeps you logged in (7 days, strictly necessary, no consent required).
- csrftoken — Security token to prevent cross-site request forgery (strictly necessary).
- django_language — Stores your language preference (functional, no consent required).
- tp_cookie_consent — Records your cookie preferences (strictly necessary).
- _ga, _ga_* — Google Analytics 4 analytics cookies (analytics, consent required, not activated until you accept via the cookie banner).

On each page load, your browser may also send your IP address to third-party CDN providers (unpkg, jsDelivr) and, if Google Fonts are loaded from Google's CDN, to Google. We are working to self-host fonts and minimize such transfers.

You can manage cookie preferences at any time via the cookie settings link in the footer.

10. Data Retention

- Account data: Retained for the duration of your account. Upon closure, deleted or anonymized within 30 days, unless retention is required by law.
- Application and project data: Retained for the duration of the relevant project plus a reasonable archive period for dispute resolution (up to 12 months after project close).
- AI interaction logs (Spotty): Retained for service quality purposes for up to 90 days, then anonymized.
- Security logs (login attempts, access logs): Retained for 90 days for fraud prevention.
- Billing records: Retained for the period required by applicable tax law (typically 10 years in Germany).
- Manual profiles and CRM contacts: Retained until you delete them or close your account.

We are implementing automated deletion and anonymization processes to enforce these periods consistently.

11. Your Rights

Under GDPR, you have the following rights:

- Right of Access (Art. 15) — Obtain a copy of the personal data we hold about you.
- Right to Rectification (Art. 16) — Correct inaccurate or incomplete data.
- Right to Erasure (Art. 17) — Request deletion of your data where it is no longer necessary or processing is unlawful. Account deletion is available via Platform settings.
- Right to Restriction (Art. 18) — Request that we limit processing in certain circumstances.
- Right to Data Portability (Art. 20) — Receive your data in a machine-readable format. A self-service data export feature is in development; in the meantime, contact service@thepending.app to request a copy of your data and we will provide it within 30 days.
- Right to Object (Art. 21) — Object to processing based on legitimate interest. Contact privacy@thepending.app.
- Right not to be subject to automated decisions (Art. 22) — Request human review of any AI-generated score or ranking that materially affects you.
- Right to Withdraw Consent — For processing based on consent (including special category data and analytics cookies), you may withdraw consent at any time without affecting the lawfulness of prior processing.

To exercise any of these rights, contact privacy@thepending.app. We will respond within 30 days. If you believe your rights have been violated, you may lodge a complaint with the Berlin data protection authority:

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Friedrichstrasse 219, 10969 Berlin | mailbox@datenschutz-berlin.de

12. Security

We implement appropriate technical and organizational measures to protect your data, including:

- Encryption in transit (HTTPS/TLS, WSS) and at rest (AWS RDS, S3, ElastiCache encryption).
- Role-based access control and object-level permission enforcement.
- CSRF protection, Content Security Policy headers, and bot detection (Cloudflare Turnstile).
- Rate-limited login with IP-based logging of authentication attempts.
- Time-limited presigned URLs for file access (1-hour expiry).
- Secrets management via AWS Secrets Manager (no hardcoded credentials).
- Webhook signature verification for all inbound webhook endpoints.

13. Manager Responsibility for Applicant and Contact Data

When managers post job openings or casting calls via the Platform, personal data of applicants is collected and processed. Managers act as the Data Controller for this applicant data. The Pending GmbH processes it as a Data Processor on the manager's behalf, as described in the Data Processing Agreement embedded in the Terms of Use (Section 9).

Managers are responsible for:

- Informing applicants of the processing of their data (e.g., via a privacy notice linked in job postings).
- Ensuring application forms do not collect unnecessary or disproportionate personal data.
- Obtaining explicit consent before collecting special category data (e.g., health conditions, physical characteristics) through custom form fields.
- Responding to data subject rights requests from their applicants and contacts.

The Pending GmbH does not independently notify applicants about data processing on behalf of managers. This is the manager's responsibility.

14. Updates to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements. The current version is always available on the Platform. We will notify registered users of material changes by email or in-platform notice.

Contact

The Pending GmbH

Arthur-Müller-Straße 24, 12487 Berlin, Germany

Email: service@thepending.app