Researcher Privacy Policy

Last updated: August 1st, 2025

1. Controller Information

1.1. Identity of the Data Controller

For the purposes of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), as well as all applicable national data protection legislation, the entity responsible for the collection and processing of your personal data in connection with the services provided via https://researcher.yubetsu.com (the "Platform") is:

Yubetsu s.r.o.
Company Registration Number: 21056064
Registered Office: Revoluční 1082/8, Nové Město, 110 00 Praha 1, Czech Republic
VAT ID: CZ21056064
Email: **legal@yubetsu.com**
Website: https://www.yubetsu.com

Yubetsu s.r.o. (hereinafter "Yubetsu", "we", "us", or "our") is the Data Controller within the meaning of Article 4(7) GDPR. This means that Yubetsu determines the purposes and means of the processing of personal data as described in this Privacy Policy.

1.2. Representative (if required under Article 27 GDPR)

If Yubetsu processes personal data of individuals located in jurisdictions outside the European Union where the appointment of a representative is legally required, such representative will be identified here or in a supplemental annexe to this Policy.

1.3. Data Protection Officer (DPO)

While Yubetsu is not currently required to appoint a Data Protection Officer under Article 37 GDPR, we voluntarily provide a dedicated point of contact for all privacy and data protection-related inquiries:

Contact for Privacy Matters:
Email: **legal@yubetsu.com**

For all inquiries, including requests related to data subject rights (access, correction, erasure, objection, etc.), please contact us at the above email address or by post at our registered office.

1.4. Supervisory Authority

If you are located in the European Economic Area (EEA) and wish to lodge a complaint regarding our handling of your personal data, you have the right to contact your local supervisory authority. Our lead supervisory authority is:

The Office for Personal Data Protection (Úřad pro ochranu osobních údajů – ÚOOÚ)
Pplk. Sochora 27
170 00 Prague 7
Czech Republic
Website: https://www.uoou.cz

You may also lodge a complaint with your national supervisory authority if you are located outside the Czech Republic but within the EEA.

2. Scope and Applicability

2.1. Material Scope

This Privacy Policy governs the collection, processing, storage, and protection of personal data in connection with your access to and use of the Platform at https://researcher.yubetsu.com, including any of its subdomains, interfaces, APIs, or affiliated digital services operated under the Yubetsu Researcher brand. It applies to all personal data that Yubetsu collects in its capacity as a Data Controller, whether directly from you or indirectly through integrations, third-party service providers, or automated means.

This Policy specifically applies to:

- Visitors to our website, regardless of whether they register;
- Registered Users, including Account holders;
- Customers purchasing Credits, subscriptions, or other paid Services;
- Users interacting with support, analytics, or AI tools provided on the Platform;
- Individuals whose personal data is processed incidentally during research, model training, feedback loops, or system usage.

2.2. Territorial Scope

This Policy applies to all individuals whose personal data is processed by Yubetsu, regardless of nationality or place of residence. However, it is specifically tailored to meet the obligations imposed by:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR);
- Act No. 110/2019 Coll., on Personal Data Processing (Czech Data Protection Act);

- The ePrivacy Directive (Directive 2002/58/EC, as amended);
- Applicable Czech and EU consumer protection and telecommunications laws.

Users outside of the EU/EEA acknowledge that their data may be transferred to and processed in the Czech Republic or other jurisdictions in accordance with the safeguards described in Section 7 (International Data Transfers).

2.3. Functional Scope

This Policy governs all processing activities performed in connection with the Platform's Services, which include but are not limited to:

- Account registration and management;
- Purchase and use of Credits or subscription plans;
- Access to data layers, reports, visualisation tools, research features, and API endpoints;
- Communication through contact forms, support tickets, or email;
- Behavioural analytics, usage monitoring, and session tracking;
- Use of cookies, pixels, and tracking technologies (further detailed in the Cookies Policy);
- AI-generated content, research simulations, and tool-based interactions.

This Policy does not apply to third-party websites, services, or integrations that may be linked to or embedded within the Platform, except to the extent that Yubetsu controls the processing of personal data shared with such third parties. We recommend reviewing the privacy terms of those external services separately (see Section 12 of the Terms and Conditions: Third-Party Services and Integrations).

3. Legal Bases for Processing

3.1. Overview

Yubetsu processes personal data lawfully, fairly, and transparently. In accordance with Article 6 of the General Data Protection Regulation (GDPR), we rely on specific legal bases depending on the context and purpose of the processing. The lawful basis for each data processing activity is determined based on necessity, proportionality, and the nature of the interaction with the Platform.

3.2. Performance of a Contract (Art. 6(1)(b) GDPR)

We process your personal data where it is necessary for the performance of a contract to which you are a party, or in order to take steps at your request prior to entering into such a contract. This includes:

- Account creation and management;
- Purchase of Credits or subscriptions;

- Enabling access to paid Services and tier-based features;
- Delivering research output, models, exports, and API responses;
- Handling billing and payment-related communications.

If you fail to provide the necessary data for contract performance, we may be unable to provide the Services.

3.3. Compliance with Legal Obligations (Art. 6(1)(c) GDPR)

We may process your personal data to comply with obligations under EU or Czech law, including but not limited to:

- Tax, accounting, and financial reporting obligations;
- Compliance with anti-money laundering (AML) and counter-terrorism laws;
- Regulatory disclosures and cooperation with public authorities or courts;
- Data retention requirements under consumer and telecommunications laws.

3.4. Legitimate Interests (Art. 6(1)(f) GDPR)

Where necessary, we process your personal data to pursue our legitimate business interests, provided such interests are not overridden by your fundamental rights and freedoms. These interests include:

- Securing, maintaining, and improving the Platform and Services;
- Fraud prevention, misuse detection, and account integrity protection;
- Statistical analysis and internal business reporting;
- Customer support and dispute resolution;
- Defending our legal rights and interests.

We conduct balancing tests before relying on legitimate interest as a basis to ensure your data rights are not infringed.

3.5. Consent (Art. 6(1)(a) GDPR)

In cases where we do not rely on another legal basis, we will seek your informed, explicit consent before processing your personal data. This includes:

- Use of optional cookies and tracking technologies (see Cookies Policy);
- Subscription to marketing communications and newsletters;
- Participation in beta testing, surveys, or research studies;
- Transfer of data to third-party tools not essential for core Services.

You may withdraw your consent at any time without affecting the lawfulness of prior processing. Where required by law, we will obtain verifiable parental consent for minors under applicable age thresholds.

3.6. Protection of Vital Interests (Art. 6(1)(d) GDPR)

In rare cases, we may process your personal data where it is necessary to protect your

vital interests or those of another natural person—such as for safety, fraud alerts, or suspected abuse scenarios requiring escalation.

4. Categories of Personal Data Collected

Yubetsu collects and processes different types of personal data depending on your relationship with the Platform, the features you use, and your specific interactions (e.g. registration, purchases, content generation, support inquiries). The data we collect is adequate, relevant, and limited to what is necessary for the purposes outlined in this Policy.

4.1. Identification and Contact Information

We collect personal information that enables us to identify or contact you directly, including but not limited to:

- Full name;
- Email address;
- Username or display name;
- Organisation name;
- Country of residence or business;
- Contact preferences;
- Communication language.

4.2. Account and Authentication Data

To provide secure access to the Platform, we collect account-related data such as:

- User ID and password (stored in hashed form);
- Account creation date;
- Login timestamps and session data;
- Authentication tokens or session identifiers;
- Verification status (e.g. verified email or organisation domain).

4.3. Payment and Transaction Data

When you purchase Credits or subscribe to paid features, we process the following information:

- Transaction amount and currency;
- Credit balance and usage history;
- Subscription tier and billing cycle;
- Payment method type (e.g. card, PayPal, invoice);
- Partial payment details (e.g. card type, masked card number);
- VAT ID (if applicable for invoicing);
- Invoices and receipts.

Note: We do not store full credit card numbers or CVV codes. Payment processing is handled securely by third-party PCI-DSS-compliant processors.

4.4. Usage Data and Platform Activity

To operate and improve our services, we automatically collect technical and usage data, including:

- Log files and timestamps of platform interactions;
- Pages visited, tools used, models queried;
- API calls and export/download activity;
- Feature usage frequency and workflow patterns;
- Preferences, settings, and tier-specific interactions;
- Crash reports and error logs (with optional diagnostics).

This data may be aggregated or pseudonymised for analytical purposes.

4.5. Device and Technical Data

We may collect device-related metadata when you access the Platform, such as:

- IP address and approximate geolocation;
- Browser type and version;
- Operating system and device model;
- Language settings;
- Referrer URLs and exit pages;
- Network type (e.g. corporate, mobile, VPN).

This helps us diagnose issues, enforce usage limits, and adapt experiences to your environment.

4.6. Communications and Correspondence

If you contact Yubetsu via email, chat, or support channels, we collect:

- The content of your messages and attachments;
- Metadata associated with the messages (timestamps, communication channel, etc.);
- Internal notes or ticket identifiers related to your inquiry;
- Follow-up status and resolution outcome.

We retain this correspondence to resolve issues, improve our support operations, and fulfil legal obligations.

4.7. User-Generated Content and Submissions

If you upload, generate, annotate, or otherwise submit content through the Platform (e.g. prompt inputs, research notes, saved models, queries, datasets), we may collect and process:

- Submission metadata (timestamps, associated user ID);

- Contents of uploads, files, text, images, or metadata;
- File structure or classification tags;
- AI model interactions and output summaries.

Such content may include personal data if you voluntarily include it. You are responsible for ensuring the lawful handling of third-party personal data in your submissions.

4.8. Optional and Sensitive Information

In rare cases where you choose to provide optional or sensitive data (e.g. special categories under Art. 9 GDPR), we will process such data only with your explicit consent or where legally required and justified, such as for diversity reporting, accessibility accommodations, or abuse investigations.

5. Purposes of Data Processing

We process your personal data only for specific, explicit, and legitimate purposes. Each processing activity is grounded in a lawful basis under the General Data Protection Regulation (GDPR) and other applicable data protection laws. The main purposes for which we collect and process your data include the following:

5.1. Account Creation and Identity Management

To register and maintain your Account on the Platform, including:

- Verifying your identity and ensuring you meet eligibility requirements;
- Managing login credentials, session control, and authentication flows;
- Enabling account recovery and contact preference settings.

Legal basis: Contractual necessity; Legitimate interest.

5.2. Provision of Services and Core Functionality

To deliver the features and functionality of the Platform, including:

- Access to research tools, datasets, dashboards, credits, and APIs;
- Enabling data submissions, processing, and export options;
- Saving and retrieving project history, custom views, or user profiles;
- Operating AI-assisted tools and generating results based on your input.

Legal basis: Contractual necessity; Legitimate interest.

5.3. Subscription Management and Payment Processing

To manage your purchase of Credits and/or subscription plans:

- Processing payments and generating invoices;
- Managing subscription status, billing cycles, and renewal notifications;

- Handling upgrades, downgrades, and balance adjustments;
- Applying tax compliance measures and maintaining accounting records.

Legal basis: Contractual necessity; Legal obligation.

5.4. Service Personalisation and User Preferences

To tailor your experience on the Platform according to your preferences:

- Remembering your display settings and language preferences;
- Recommending features based on usage history;
- Adjusting UI components and accessibility settings;
- Adapting content delivery based on your selected plan or region.

Legal basis: Legitimate interest; Consent (for certain cookies or trackers).

5.5. Technical Operation, Maintenance, and Security

To ensure the proper operation, availability, and security of the Platform:

- Monitoring system performance and usage metrics;
- Detecting and preventing abuse, fraud, or unauthorised access;
- Applying rate limits and usage controls;
- Conducting audits, backups, and system diagnostics.

Legal basis: Legitimate interest; Legal obligation.

5.6. Communication and Customer Support

To communicate with you about your account, services, and support inquiries:

- Responding to technical, billing, or legal inquiries;
- Sending service-related announcements or disruption notices;
- Following up on feedback, tickets, or reported issues;
- Providing onboarding, usage tips, or product updates.

Legal basis: Contractual necessity; Legitimate interest.

5.7. Analytics, Research, and Product Improvement

To understand how users interact with the Platform and improve our offerings:

- Analysing user flows, feature usage, and content performance;
- Aggregating feedback and usage patterns for internal research;
- Testing new features, layouts, or AI models;
- Generating anonymised or pseudonymized usage reports.

Legal basis: Legitimate interest; Consent (where applicable).

5.8. Legal Compliance and Regulatory Obligations

To comply with applicable laws, regulations, and lawful requests:

- Retaining certain records for tax and accounting compliance;

- Assisting with law enforcement or regulatory investigations;
- Preventing, detecting, and reporting suspected fraud or criminal behaviour;
- Enforcing our Terms and defending against legal claims.

Legal basis: Legal obligation; Legitimate interest.

5.9. Marketing and Outreach (Limited Use)

To inform Users of new features, events, or educational resources:

- Sending email newsletters or platform tips (with opt-out option);
- Inviting users to participate in surveys or feedback sessions;
- Promoting relevant upgrades or partner services based on usage context.

Legal basis: Consent (where required); Legitimate interest (limited scope, with opt-out).

6. How We Collect Data

We collect personal data through various methods depending on how you interact with the Platform. The data we gather originates from the following primary sources:

6.1. Directly from Users

We collect data directly from you when you voluntarily provide it to us. This occurs in contexts where you actively engage with the Platform, including but not limited to:

- Creating or updating an account;
- Completing forms or fields during onboarding or profile setup;
- Subscribing to a plan or purchasing Credits;
- Submitting payment information during a transaction;
- Contacting support, providing feedback, or submitting a request;
- Posting content, uploading files, or using research tools that require input;
- Participating in surveys or usability testing, where applicable.

Such data may include identification information (e.g., name, email address), authentication credentials, billing details, organisation name, user-submitted content, and communication records.

6.2. Automatically Through Technical Means

When you access or interact with the Platform, we automatically collect certain data using technical and analytics tools. This collection helps us ensure system integrity, optimise user experience, detect fraud, and understand usage patterns. This includes:

- Device and browser identifiers (e.g., IP address, user-agent string, device model);
- Log data (e.g., access times, URLs visited, error reports);
- Platform usage metadata (e.g., feature usage, API calls, clickstream data);

- Session and performance tracking (e.g., session duration, latency metrics);
- Cookies and tracking pixels, subject to your consent preferences.

This data is collected using technologies such as cookies, local storage, log files, and third-party analytics tools. For more information, see our Cookies Policy.

6.3. From Third-Party Sources

We may also receive personal data from external partners, service providers, or integrations you interact with. These include:

- Authentication and identity providers, such as when you log in using social accounts or single sign-on (SSO) systems (e.g., Google, GitHub, ORCID);
- Payment processors, who securely transmit billing and transaction information related to Credit purchases or subscriptions (e.g., Stripe, PayPal);
- Analytics and feedback platforms, which may deliver pseudonymized usage and event data;
- Affiliated services or platforms, when you access the Platform through an enterprise or institutional license.

We take appropriate measures to ensure that such third-party sources are GDPR-compliant and only provide data with a legitimate basis or user consent where required.

7. Data Sharing and Disclosure

We are committed to protecting your personal data and only share it with trusted third parties under specific, lawful circumstances. We do not sell or rent your personal data to any third parties for marketing or commercial purposes. The following outlines the limited scenarios in which your data may be shared:

7.1. With Subprocessors and Third-Party Service Providers

We engage trusted subprocessors and third-party service providers who perform services on our behalf or assist in operating the Platform. These include, but are not limited to:

- Cloud hosting providers (e.g., Amazon Web Services, Microsoft Azure) for secure infrastructure and data storage;
- Payment processors (e.g., Stripe, PayPal) for handling billing and transactions;
- Analytics services (e.g., Plausible, Matomo, or other GDPR-compliant tools) for usage analysis and feature optimisation;
- Email and communication platforms (e.g., Mailgun, Postmark) for transactional messaging;
- Customer support platforms (e.g., Intercom, Zendesk) to facilitate issue tracking and response.

All subprocessors are contractually bound by Data Processing Agreements (DPAs) and are required to comply with data protection obligations equivalent to those under the GDPR, including data security, confidentiality, and limited processing purposes.

7.2. With Regulatory Authorities and Law Enforcement

We may disclose your personal data if required to do so by law, or in the good-faith belief that such action is necessary to:

- Comply with legal obligations or valid legal processes (e.g., court order, subpoena);
- Cooperate with law enforcement or regulatory investigations;
- Prevent or investigate suspected fraud, abuse, or illegal activities;
- Protect the rights, safety, or property of Yubetsu, its Users, or the public.

Any such disclosure will be limited to what is strictly necessary and, where legally permissible, we will notify you of such requests.

7.3. In Business Transfers

In the event of a corporate transaction involving Yubetsu, such as a merger, acquisition, asset sale, restructuring, or bankruptcy, your personal data may be disclosed or transferred as part of the transaction, subject to appropriate confidentiality obligations. Should such a transfer occur, we will take steps to ensure that the receiving party processes your data in a manner consistent with this Privacy Policy and applicable data protection laws.

7.4. No Sale or Commercial Disclosure of Personal Data

Yubetsu does not sell, trade, or otherwise monetise your personal data. We do not share your personal information with advertisers or data brokers. Any sharing of personal data is limited to service provision, compliance, and operational requirements as described above.

8. International Transfers

Due to the global nature of our operations and technology infrastructure, your personal data may be transferred to and stored or processed in countries outside of your jurisdiction, including jurisdictions that may not offer the same level of data protection as those within the European Economic Area (EEA). We remain committed to ensuring that such transfers are conducted in compliance with applicable data protection laws, particularly the General Data Protection Regulation (GDPR).

8.1. Information on Data Storage Locations

Personal data collected through the Platform may be stored and processed on servers located in multiple jurisdictions. Our primary infrastructure is hosted on servers in the

United States. Additionally, certain subprocessors and service providers may process data in other jurisdictions to provide redundancy, failover, or regional services.
We select infrastructure partners with a strong record of compliance and data security. Data storage locations may include, but are not limited to:

- United States
- European Union (for certain high-sensitivity data sets, subject to user configuration or applicable legal requirements)

8.2. Use of U.S.-Based Subprocessors

Some of the services essential to the operation of the Platform are provided by subprocessors located in the United States. While these subprocessors may process personal data on our behalf, Yubetsu ensures that any such transfers are conducted in full compliance with applicable data protection regulations.

To safeguard user privacy:

- All subprocessors are contractually bound by robust data processing agreements incorporating Standard Contractual Clauses (SCCs) approved by the European Commission.
- Where appropriate, we implement supplementary measures—including encryption, data minimisation, and strict access controls—to mitigate any risk associated with non-EEA data processing.
- We conduct due diligence and risk assessments for all subprocessors handling personal data, ensuring that their privacy practices align with our legal obligations and security standards.

Despite differences in jurisdiction, we maintain a high level of protection for your data regardless of where it is processed.

9. Data Retention

Yubetsu retains personal and operational data for periods consistent with the nature and purpose of the processing, applicable legal obligations, and legitimate business interests. The duration for which specific data is retained depends on several factors, including the category of data, user account status, frequency of access, and relevant regulatory requirements.

9.1. Account-Linked Data

Personal information associated with a User's Account—including contact details, authentication credentials, billing history, and support correspondence—is generally retained for as long as the Account remains active. Upon deletion or deactivation of an

Account, certain data may be retained for a limited period for dispute resolution, legal compliance, fraud prevention, or to satisfy tax or financial recordkeeping obligations as permitted or required under applicable law.

9.2. Operational Archives

In order to support the integrity, continuity, and progressive development of the Platform, Yubetsu maintains secure archives of anonymised and pseudonymized outputs generated through automated research utilities, intelligent agents, and dynamic document generation systems. These outputs, which may include large-language model interactions and automated content processing results, are periodically reviewed in aggregate form for purposes such as system calibration, academic benchmarking, and research trend monitoring. These archives are maintained independently of user-identifiable data and are not automatically purged following individual account deletion.

9.3. Digest and Aggregation Services

Daily, curated summaries and digests of academic, technical, and domain-specific literature—processed and delivered via automated means—may be stored in long-term repositories to facilitate future analysis, recommender system optimisation, and retrospective metadata studies. These content aggregates do not constitute personal data under applicable law and are retained at Yubetsu's discretion for strategic and research-supporting purposes.

9.4. Minimisation and Retention Review

Yubetsu adheres to the principle of data minimisation. Data that no longer serves a valid operational or legal purpose is periodically reviewed and securely deleted or anonymised. Retention schedules and review procedures are documented internally and assessed in light of applicable data protection frameworks, including GDPR Article 5(1)(e).

10. Your Rights Under GDPR

If you are located in the European Economic Area (EEA), the United Kingdom, Switzerland, or are otherwise subject to the GDPR, you have the following rights regarding your personal data processed by Yubetsu:

- **Right to access personal data**
- You may request confirmation of whether we process your personal data and obtain a copy of the data, along with information about the purposes, categories, and recipients of the processing.
- **Right to rectification**
- You can request correction of inaccurate or incomplete personal data held about you.

- **Right to erasure (“right to be forgotten”)**
- You may request deletion of your personal data where it is no longer necessary for the purposes for which it was collected, where you have withdrawn consent, or where the data was unlawfully processed. Certain data may be retained in accordance with legal or operational requirements (see Section 9).
- **Right to restrict processing**
- You can request that we temporarily or permanently suspend processing of your personal data under specific conditions, such as during the review of an objection or while verifying data accuracy.
- **Right to erasure (“right to be forgotten”)**
- You may request deletion of your personal data where it is no longer necessary for the purposes for which it was collected, where you have withdrawn consent, or where the data was unlawfully processed. Certain data may be retained in accordance with legal or operational requirements (see Section 9).
- **Right to restrict processing**
- You can request that we temporarily or permanently suspend processing of your personal data under specific conditions, such as during the review of an objection or while verifying data accuracy.
- **Right to data portability**
- You are entitled to receive a copy of your personal data in a structured, commonly used, and machine-readable format and have the right to transmit that data to another controller, where technically feasible.
- **Right to object to processing**
- You may object to our processing of your personal data based on legitimate interests or for direct marketing purposes. Upon objection, we will cease processing unless we demonstrate compelling legitimate grounds.
- **Right to withdraw consent at any time**
- Where processing is based on your consent, you may withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing prior to withdrawal, but may impact your continued use of some Services.
- **Right to lodge a complaint with a supervisory authority**
- You may lodge a complaint with a data protection authority in the country of your residence or the location of the alleged violation. For users in the Czech Republic, this is:

Úřad pro ochranu osobních údajů (ÚOOÚ)
Pplk. Sochora 27, 170 00 Praha 7
https://www.uoou.cz

11. Security Measures

Yubetsu maintains a comprehensive set of administrative, technical, and organisational safeguards to protect your personal data from unauthorised access, loss, alteration, or disclosure. These measures reflect the sensitivity of the data and the evolving nature of security threats.

11.1. Technical and Organisational Safeguards

We implement industry-standard security protocols to ensure the confidentiality, integrity, and availability of personal data. These include:

- End-to-end encryption for data in transit and at rest
- Role-based access control (RBAC) and multifactor authentication (MFA)
- Pseudonymisation and data minimisation practices
- Network isolation, secure logging, and continuous monitoring
- Regular vulnerability scanning, patching, and infrastructure hardening

11.2. Incident Response and Breach Notification

Yubetsu maintains an internal incident response plan that outlines procedures for identifying, containing, and remediating security incidents. In the event of a personal data breach that poses a risk to individuals' rights and freedoms, we will notify affected users and competent supervisory authorities without undue delay, in accordance with legal requirements.

11.3. Staff Confidentiality and Training

All personnel with access to personal data are bound by contractual confidentiality obligations and are trained regularly on data protection principles, information security, and secure development and handling practices. Access to data is strictly limited to those with a legitimate business need.

12. Cookies and Similar Technologies

Yubetsu uses cookies and similar tracking technologies to enhance the user experience, analyse usage patterns, and ensure the functionality and security of the Platform. These technologies may collect certain data automatically when you interact with our Services.

12.1. Types of Cookies and Tracking Technologies Used

We use a combination of the following technologies:

- Strictly Necessary Cookies: Essential for the operation of the Platform (e.g., session identifiers, security tokens).

- Performance and Analytics Cookies: Help us understand how users interact with the Platform, enabling us to improve functionality and user experience (e.g., page load metrics, navigation behaviour).
- Functional Cookies: Allow us to remember user preferences, such as language or region settings.
- Optional Tracking Tools (if enabled): May include anonymised third-party analytics tools. No advertising cookies are deployed unless explicitly stated or consented to.

We do not use behavioural advertising technologies or cross-site tracking for marketing purposes without your explicit opt-in consent.

12.2. Cookie Preferences and Control

You can manage or disable cookies through your browser settings or via our in-app cookie management interface, where available. Certain features of the Platform may not function properly if cookies are disabled.

12.3. Link to Full Cookies Policy

For detailed information on the types of cookies we use, their purposes, and how to manage your preferences, please see our full https://researcher.yubetsu.com/legal/cookies-policy.

13. Children's Privacy

Yubetsu is committed to protecting the privacy of minors and ensuring that the Platform is used responsibly by individuals of appropriate age.

13.1. Age Restriction

The Platform and Services are not intended for, and may not be used by, individuals under the age of 18. By accessing or using Yubetsu, you affirm that you are at least 18 years old or the legal age of majority in your jurisdiction, whichever is higher.

13.2. No Intentional Collection of Data from Minors

We do not knowingly collect or solicit personal data from individuals under 18. If we become aware that we have inadvertently received personal information from a minor without appropriate parental or guardian consent, we will take reasonable steps to delete such data as soon as possible.

14. Policy Updates and Revisions

Yubetsu reserves the right to update, amend, or modify this Privacy Policy at any time to reflect changes in our practices, legal requirements, or technological advancements.

14.1. Communication of Changes

Significant updates to this Privacy Policy will be communicated to Users through prominent notifications on the Platform, via email where applicable, or through other reasonable means. Continued use of the Platform following such updates constitutes your acceptance of the revised Privacy Policy.

14.2. Date of Last Revision

The effective date of the current Privacy Policy is indicated at the top of this document. Users are encouraged to review the Privacy Policy periodically to stay informed of any changes.

15. Contact Information

For any questions, concerns, or requests regarding your privacy or personal data processed by Yubetsu Researcher, you may contact us directly.

15.1. Email for Privacy Inquiries and Data Requests

Please send all privacy-related inquiries, including requests for access, correction, or deletion of your personal data, to our dedicated privacy email address: legal@yubetsu.com.

15.2. Physical Mailing Address

You may also contact us by mail at the following address for any privacy matters or formal requests:

Yubetsu s.r.o.
Revoluční 1082/8
110 00 Prague 1
Czech Republic