Privacy Policy

Canonical online PDF URL:
https://pdfdata.org/legal/privacy-policy.pdf

Materials PDF Database - Privacy Policy (English Version)

Tongji University Yang Group

Effective Date: January 1, 2026

The Materials PDF Database (the "Database") is a research project of the Tongji University Yang Group ("Yang Group," "we," "us," or "our"). This Privacy Policy (the "Policy") explains how we collect, use, store, and disclose your personal information when you access or use the Database website and any website, application, or service that links to this Policy (collectively, the "Service"). It also explains your rights and choices with respect to your personal information.

By using the Service, you consent to the collection and processing of your personal information as described in this Policy. This Policy forms part of the Terms of Use for the Service.

I. Information We Collect

1. Information You Provide to Us

When you access or use the Service, for example when you:

- log in to or register an account;
- upload data, run analyses, or use any feature of the Service;
- send us questions, feedback, or collaboration requests;

we collect personal information that you voluntarily provide, including without limitation:

(1) Personal identifiers
Such as your name, username, IP address, and other unique identifiers.

(2) Contact details
Such as your email address and telephone number.

(3) Account and usage information
Such as login records, service usage logs, actions you initiate (uploads, downloads, processing tasks, etc.), and other activity information associated with your account.

(4) Professional / academic information
Such as your institution or organization, school or department, position, title, research field or interests, and academic status.

(5) Educational information
Such as educational background or related education information that you choose to provide in your profile or communications.

(6) Information you choose to upload to a third-party open repository (Zenodo)
When you choose the "Upload/Publish to Zenodo" feature in the Service, we will submit the data files you select and their related metadata to the Zenodo platform according to your instructions. Submitted content typically includes:

the files you choose to upload; descriptive metadata related to those files (for example, material name, author, and affiliated institution, as reflected in the information you enter or confirm in the upload interface); and the technical information and operation records necessary to complete the upload and link the record (such as upload time and record ID).

Please note:

Zenodo is an open research-output repository operated by CERN and others. After publication, a record is typically assigned a DOI and may be visible to the public.

After a record is published, deletion or withdrawal may be limited. Zenodo may retain a tombstone page to ensure citations remain valid, and may retain identifiers such as DOI/URL.

Zenodo does not provide data anonymization services. You should ensure that uploaded content does not contain personal information, sensitive information, or restricted data that you are not authorized to disclose. You are solely responsible for any third-party dispute or compliance risk arising from your uploads.

When you choose to use this feature, you understand and agree that, for the purpose of completing the upload/publication, the Service will transmit the above information to Zenodo and that Zenodo/CERN terms and privacy notices will apply.

2. Information We Obtain from Third Parties
When you choose to log in with a third-party account (such as GitHub or ORCID) and complete authorization, we obtain from that third party, within the scope of authorization you confirm on the third-party platform, the information necessary for login and account linking, such as your name (if any), email address, username, avatar, and institution information. We combine that information with the information you provide directly through the Service to open, link, and manage your account and to enable login, identity verification, and related functionality.

3. Information Collected Automatically
When you access or use the Service, we automatically collect the following technical and usage information through server logs and similar technologies to maintain the security and stability of the Service and conduct basic statistical analysis:

(1) Device and network identifiers
Such as IP address, browser type, operating system, and device type.

(2) Usage information
Such as the date and time of access, pages or features visited, actions performed (uploads, processing, visualization, etc.), and error logs.

This information is used to maintain the security and performance of the Service and to continually improve its functionality.

II. Online Identification Technologies
We may use LocalStorage or other similar technologies (such as pixel tags and web beacons) to:

- maintain your login status (for example, by storing access tokens / session identifiers);
- remember your preferences and session information;
- prevent duplicate submissions and improve service stability and security;
- conduct necessary operational analysis and troubleshooting to improve performance and user experience.

You may clear locally stored data or disable related storage permissions in your browser settings, but doing so may require you to log in again or may cause some features not to function properly.

After you finish using the Service, you may also manually clear your browser cache, local storage, and cookie data. We do not use third-party advertising-tracking cookies and do not share your identifiers with third parties for advertising purposes (unless otherwise disclosed and consented to).

III. How We Use Your Personal Information
We may process your personal information for the following purposes:

1. Identification and authentication
Use scenario: when you register, log in, remain logged in, retrieve or change account information, or undergo security verification.

Information processed: email address / username, user ID, login and session information, IP address, and device and browser information for security verification and risk control.

2. Providing and operating the Service
Use scenario: when you use account management, data upload, analysis/processing, visualization, download, and similar functions.

Information processed:

Account information: email address / username and user ID;

Basic uploaded material information that you provide: for example, metadata fields in the upload form such as material name, test station / beamline, and affiliated institution / unit (as completed and submitted by you), used to create data records, support indexing and retrieval, display information, and enable subsequent processing;

Service usage records: records of the actions you initiate (uploads, downloads, processing tasks, etc.) and task-related status information (task start/end time, running status, error information, etc.), used to provide task management and return results to you.

3. Communicating with you
Use scenario: when you send us inquiries, feedback, or collaboration requests, or when we send you important notices relating to service security, feature changes, or policy updates.

Information processed: contact information (email address; telephone number only if you provide it and only for contact purposes), communication content, and related log information necessary to locate issues (limited to what is necessary).

4. Academic research and development
As part of the research work of the Tongji University Yang Group, during operation of the Service we internally use the contents of files you upload and their accompanying metadata to support academic research and the development, testing, and quality improvement of systems/algorithms, including without limitation the development and optimization of parsing and processing algorithms, the design and validation of benchmark datasets and evaluation tasks, and data quality assessment, anomaly detection, and format-compatibility improvements.

Information processed: files you upload (such as .gr, .iq, .sq, .fq, .cif, and accompanying files);

Metadata you submit (for example, material name, test station / beamline, affiliated institution / unit, and other fields you complete and submit in the upload form). In conducting the above research and development, we do not aim to identify your real-world identity and, where possible, use relevant data internally in de-identified, masked, or aggregated form while controlling access permissions and scope of use.

5. Protection of rights and compliance with legal requirements
Use scenario: when detecting, preventing, and handling service abuse, security incidents, fraud, or violations of the Terms of Use, and when cooperating with regulatory or judicial authorities as required by law.

Information processed: account identifiers (user ID, email address / username), access and operation logs (including IP address, device and browser information, request frequency, abnormal activity records, etc.), and necessary evidence materials related to incident handling.

We may process your data on the following legal bases: your consent, necessity for performance of our agreement with you, and compliance with legal requirements. De-identified, anonymized, or aggregated information is not subject to this Policy.

IV. When We Share Your Personal Information
We do not sell your personal information. We share information only in the following circumstances:

1. Within Tongji University
We may share information with other research or administrative departments of the university for internal research, service operation, analysis, or security management.

2. Service providers and technical partners
We may share necessary information with third-party vendors, such as server hosting providers, authentication services, security tools, and analytics tools. Third-party vendors may use the information only as instructed by us and for no other purpose.

3. Content you choose to make public
Some Service features may allow you to display your name, institution, contribution records, and similar information to other users. The relevant scope of disclosure will be explained in the applicable feature.

4. Academic collaboration and research outputs
We may provide de-identified data to collaborating scholars or use aggregated data in academic papers and research presentations.

5. Protection of rights and safety
We may disclose information when we believe it is necessary to protect the safety of the Yang Group, the university, users, or the public, such as in the investigation of violations or unlawful conduct.

6. Legal requirements
We may disclose information as required by courts, regulators, or law-enforcement authorities in accordance with law.

If, in the future, the Service is transferred to another department of Tongji University due to organizational restructuring, your information may be transferred within the university and will remain subject to appropriate protective measures.

V. Your Rights
To the extent permitted by applicable law, you may have the following rights:

- to request access to the personal information we hold about you;
- to request correction of inaccurate or incomplete information;
- to request deletion of your information, where applicable;
- to object to or restrict certain processing activities;
- to withdraw consent at any time where processing is based on consent (without affecting the lawfulness of processing before withdrawal).

If you wish to exercise the above rights, please contact us using the contact details at the end of this Policy. We may need to verify your identity.

You may also have the right to lodge a complaint with a data protection authority in your place of residence. We encourage you to contact us first so that we can help address your concern.

VI. Cross-Border Data Transfers
The Service primarily operates and stores data within the People's Republic of China. However, in the context of international cooperation or the use of cross-border technical services, your information may be accessed from or transferred to other countries or regions.

We will take reasonable measures to ensure that applicable safeguards meet relevant legal requirements and that your data receives a level of protection comparable to that of your location.

VII. Information of Minors
The Service is intended for adults with a research or academic background and is not directed to children. We do not knowingly collect information from persons under 18 years of age.

If you believe that a minor has provided us with information, please contact us and we will address the matter promptly.

VIII. Third-Party Links
The Service may contain links to third-party websites or tools. This Policy applies only to services operated by us. When you visit a third-party website, its privacy practices will be governed by its own privacy policy.

IX. Data Retention
We retain your information for the following periods or purposes:

- maintaining your account;
- supporting ongoing research and system improvement;
- complying with legal obligations;
- resolving disputes and enforcing the Terms of Use.

After our relationship with you ends, we will retain only the information necessary for legal compliance or research-archive preservation purposes, after which it will be deleted or anonymized.

X. Information Security
We value the security of your personal information and, in light of the actual circumstances of the Service, adopt technical and managerial measures appropriate to the risk to protect your personal information. However, please understand that no security measure on the internet is absolute.

Transmission security measures

We transmit data using HTTPS/TLS encryption protocols to reduce the risk of unauthorized access, interception, or tampering during network transmission. Access tokens generated after account login (such as JWT tokens) are transmitted between the front end and back end through encrypted channels and are verified by server-side signatures and expiration checks to prevent forgery or misuse.

Identity authentication and session management

We authenticate users through a combination of account credentials and access tokens, set reasonable token validity periods and refresh strategies, and may invalidate tokens when abnormal activity is detected. The front end stores access tokens and other information necessary to maintain login status in the browser's localStorage or sessionStorage, but we do not store your account password in plain text on the client side. We also recommend that you log out promptly after use and clear related local data.

Access control and the principle of least privilege

For backend systems involving personal information and business data, we implement account hierarchy and access control, authorizing only personnel who need access to perform their duties and only within the appropriate permission scope. We also record logs of important operations and access activities so that necessary security audits and issue investigations can be conducted.

Data storage and backup protection

We do not set a login password. Users log in using a one-time verification code sent to their email address. The verification code is used only for short-term identity verification and session establishment and is not retained long-term in the system. To protect your personal information and business data, servers storing relevant data employ access control, system hardening, and regular security patch updates to reduce the risk of unauthorized access, malicious attacks, and data leakage. At the same time, we perform regular backups of key data as business needs require and apply corresponding access restrictions and security management measures to backup data to prevent unauthorized access, tampering, or misuse.

Security monitoring and incident response

We monitor behavior that may affect the security and stable operation of the system through access logs, error logs, and abnormal behavior detection mechanisms, such as unusually frequent requests, unusual login attempts, or suspected malicious scraping. Depending on the circumstances, we may apply rate limits, temporarily restrict access, or block accounts. If we discover a security incident involving actual or potential leakage, tampering, or loss of personal information, we will initiate an emergency response in accordance with laws, regulations, and regulatory requirements, take remedial measures, and notify you and the competent authorities where required.

Your security responsibilities

Although we have taken reasonable and necessary security measures, the transmission and storage of information on the internet still involve risks. You should properly safeguard your account and login credentials, not disclose them to others, and avoid remaining logged in for extended periods on untrusted devices or networks. If you discover that your account may have been compromised, or that abnormal login or activity has occurred, please contact us promptly using the contact details provided in this Policy, and we will assist you in taking appropriate protective measures.

XI. Policy Updates

We may update this Policy from time to time. If there are material changes, we will update the "Effective Date" and may provide additional notice, such as an in-service announcement or email notice.

Your continued use of the Service constitutes acceptance of the updated Policy.

XII. Contact Us

If you have any questions about this Policy, please contact us:

Tongji University Yang Group (https://www.yanglonggroup.com)

Address: Tongji University, 4800 Cao'an Highway, Jiading District, Shanghai, People's Republic of China

Email: long_yang@tongji.edu.cn

材料 PDF 数据库 - 隐私政策（中文版）

同济大学杨龙课题组

生效日期：2026 年 1 月 1 日

材料 PDF 数据库（Materials PDF Database）（以下简称“本数据库”）是同济大学杨龙课题组（（Tongji University Yang Group）以下简称“杨龙课题组”“我们”）的研究项目。本隐私政策（“本政策”）说明当您访问或使用本数据库网站及任何链接至本政策的网站、应用程序或服务（统称为“本服务”）时，我们如何收集、使用、存储和披露您的个人信息。本政策也说明您就您的个人信息所享有的权利与选择。

您使用本服务即表示您同意按照本政策所述方式收集和处理您的个人信息。本政策是本服务《使用条款》的组成部分。

一、我们收集的信息

1. 您主动提供给我们的信息

当您访问或使用本服务时，例如：

- 登录或注册账户；
- 上传数据、运行分析或使用本服务的任何功能；
- 向我们发送问题、反馈或合作请求；

我们会收集您主动提供的个人信息，包括但不限于：

（1）个人标识信息

如您的姓名、用户名、IP 地址以及其他唯一识别标识。

（2）联系方式

如您的电子邮箱、电话号码。

（3）账户及使用信息

如登录记录、服务使用日志、您发起的操作（上传、下载、处理任务等），以及与您的账户关联的其他活动信息。

（4）专业 / 学术信息

如您的所属机构或组织、学院或部门、职务、职称、研究领域或研究兴趣、学术身份等。

（5）教育信息

如您选择在个人资料或沟通中提供的学历背景或相关教育信息。

（6）选择上传至第三方开放仓储（Zenodo）的信息

当您在本服务中选择“上传/发布至 Zenodo”功能时，我们将根据您的指令把您选定的数据文件及其相关元数据提交至 Zenodo 平台。提交内容通常包括：

您选择上传的文件本体；与该文件相关的描述性元数据（例如材料名称、作者、所属机构等，具体以您在上传界面填写或确认的信息为准）；为实现上传与记录关联所必需的技术信息与操作记录（如上传时间、记录 ID 等）。

请注意：

Zenodo 是由 CERN 等机构运营的开放研究成果仓储，上传发布后通常会为记录分配 DOI，并可能对公众可见。

记录发布后，删除或撤回可能受到限制：Zenodo 可能保留“墓碑页（tombstone page）”以确保引用不失效，并保留 DOI/URL 等标识信息。

Zenodo 不提供数据匿名化服务。您应确保上传内容不包含您无权披露的个人信息、敏感信息或受限制数据；如因您上传内容引发第三方争议或合规风险，责任由您自行承担。

当您选择使用该功能时，意味着您理解并同意：为完成上传/发布目的，本服务会将上述信息传输至 Zenodo，并适用 Zenodo/CERN 的相关条款与隐私声明。

2. 我们从第三方获得的信息

当您选择使用第三方账号登录（如 GitHub 或 ORCID）并完成授权时，我们会根据您在第三方平台确认的授权范围，从该第三方获得与登录和账号绑定所必需的信息，例如姓名（如有）、电子邮箱、用户名、头像、机构信息等。我们将上述信息与您在本服务中直接提供的信息结合，用于为您开通、绑定和管理账户，并实现登录、身份识别和相关功能。3. 自动收集的信息

当您访问或使用本服务时，我们会通过服务器日志等技术手段自动收集以下技术和使用信息，用于保障服务的安全性、稳定性和基础统计分析：

（1）设备和网络标识

如 IP 地址、浏览器类型、操作系统、设备类型。

（2）使用信息

如访问日期与时间、访问的页面或功能、执行的操作（上传、处理、可视化等）、错误日志等。

这些信息用于保障服务的安全性、性能，并持续改进服务功能。

二、在线识别技术

我们可能使用 LocalStorage 或其他类似技术（如像素标签、web beacon）用于：

- 维持您的登录状态（例如保存访问令牌/会话标识）；
- 记住您的偏好设置与会话信息；
- 防止重复提交、提升服务稳定性与安全性；
- 进行必要的运行分析与故障排查，以改进性能和用户体验。

您可以在浏览器设置中清除本地存储数据或禁用相关存储权限；但这可能导致您需要重新登录，或部分功能无法正常使用。使用结束后，您也可以手动清除浏览器缓存、本地存储与 Cookie 数据。我们不使用第三方广告追踪类 Cookie，也不会基于广告目的向第三方共享您的标识信息（除非另行明示并取得同意）

三、我们如何使用您的个人信息

我们可能基于以下目的处理您的个人信息：

1. 身份识别与认证

使用场景： 您注册、登录、保持登录状态、找回或变更账户信息、进行安全校验时。

处理的信息： 电子邮箱/用户名、用户 ID；登录与会话信息；IP 地址；设备与浏览器信息，用于安全校验与风控。

2. 提供与运营服务

使用场景： 您使用账户管理、数据上传、运行分析/处理、可视化展示、下载等功能时。

处理的信息：

账户信息： 电子邮箱/用户名、用户 ID；

上传材料基本信息（您主动填写）： 例如材料名称、测试线站/光束线（beamline）、所属机构/单位等上传表单中的元数据字段（以您填写/提交为准），用于建立数据条目、索引检索、展示与后续处理；

服务使用记录： 您发起的操作记录（上传、下载、处理任务等）及与任务相关的状态信息（任务开始/结束时间、运行状态、错误信息等），用于为您提供任务管理与结果返回。

3. 与您沟通

使用场景： 您向我们发送咨询、反馈或合作请求，或我们向您发送与服务安全、功能变更、政策更新相关的重要通知时。

处理的信息： 联系方式（电子邮箱；如您提供电话亦仅用于联系）；沟通内容；为定位问题所必需的相关日志信息（仅限必要范围）。

4. 学术研究与开发

作为同济大学杨龙课题组开展科研工作的一部分，我们会在服务运行过程中，将您上传的文件内容及其配套元数据，在内部用于支持学术研究与系统/算法的开发、测试和质量改进，包括但不限于：解析与处理算法的开发与优化；基准数据集与评测任务的设计与验证；数据质量评估、异常检测与格式兼容性改进。

处理的信息：您上传的文件（如 .gr、.iq、.sq、.fq、.cif 及其配套文件）；

您提交的元数据（例如材料名称、测试线站/光束线、所属机构/单位，以及上传表单中您填写/提交的其他字段）。我们在开展上述研究与开发时，不以识别您的现实身份为目的，并会尽可能以去标识化、脱敏或汇总的方式在内部使用相关数据，控制访问权限与用途范围；

5. 权利保护与符合法律要求

使用场景： 检测、预防和处理服务滥用、安全事件、欺诈或违反《使用条款》的行为；以及依法配合监管、司法机关要求时。

处理的信息： 账户识别信息（用户 ID、邮箱/用户名）；访问与操作日志（含 IP、设备与浏览器信息、请求频率、异常行为记录等）；与事件处置相关的必要证据材料。

我们可能基于以下法律依据处理您的数据：您的同意、履行与您的协议所必需以及符合法律要求。经去标识、匿名化或汇总的信息不受本政策限制。

四、我们何时共享您的个人信息

我们不会出售您的个人信息。我们仅在下列情况下共享信息：

1. 同济大学内部

可能与学校其他研究部门或管理部门共享，用于内部研究、服务运行、分析或安全管理。

2. 服务提供商与技术合作方

我们可能向第三方供应商共享必要信息，如服务器托管、认证服务、安全工具、分析工具等。第三方供应商仅可按我们的指示使用信息，不得进行其他用途。

3. 用户选择公开的内容

部分服务功能可能允许您向其他用户展示姓名、机构、贡献记录等。该公开范围会在具体功能中说明。

4. 学术合作与科研输出

我们可能向合作学者提供去标识数据，或在学术论文、研究展示中使用汇总数据。

5. 权利与安全保护

当我们认为必要时，可披露信息以保护杨龙课题组、学校、用户或公众的安全，例如调查违规或违法行为。

6. 法律要求

如法院、监管机构、执法部门要求，我们可能依法披露信息。

如未来服务因组织结构调整而转移至同济大学其他部门，您的信息可能在校内转移，并被采取适当保护措施。

五、您的权利

在适用法律允许范围内，您可能享有以下权利：

- 请求访问我们持有的您的个人信息；
- 请求更正不准确或不完整信息；
- 请求删除您的信息（在适用情形下）；
- 反对或限制部分处理活动；
- 在基于同意处理时，您可随时撤回同意（不影响撤回前的处理合法性）。

如需行使上述权利，请使用本政策末尾的联系方式联系我们，我们可能需要验证您的身份。

您也可能有权向您所在地的数据保护机构提出投诉。我们鼓励您先联系我们以便协助解决。

六、跨境数据传输

本服务主要在中华人民共和国境内运行和存储数据。但在国际合作或使用跨境技术服务的情况下，您的信息可能被访问或传输至其他国家或地区。

我们将采取合理措施，确保适用的保护措施符合相关法律要求，确保您的数据获得与您的所在地相当的保护水平。

七、未成年人信息

本服务面向具有科研或学术背景的成年人，不面向儿童。我们不会主动收集 18 岁以下未成年人的信息。

如您认为未成年人向我们提供了信息，请联系我们，我们将及时处理。

八、第三方链接

本服务可能包含指向第三方网站或工具的链接。本政策仅适用于我们运营的服务。您访问第三方网站时，其隐私实践将适用其自身的隐私政策。

九、信息保留

我们将在以下期间保留您的信息：

- 维持您的账户；
- 支持持续研究与系统改进；
- 遵守法律义务；
- 解决争议、执行使用条款。

在关系结束后，我们仅会在法律要求或科研档案保存目的下继续保留必要信息，其后将删除或匿名化。

十、信息安全

我们重视您的个人信息安全，并结合本服务的实际情况，采取与风险相适应的技术和管理措施保护您的个人信息，但也请您理解，互联网环境下不存在绝对安全。

传输安全措施

我们通过 HTTPS/TLS 加密协议传输数据，以降低数据在网络传输过程中被未授权访问、截获或篡改的风险。账户登录后生成的访问令牌（如 JWT token）在前后端交互时通过加密通道传输，并在服务端进行签名与有效期校验，以防止被伪造或篡用。

身份认证与会话管理

我们通过账户密码结合访问令牌的方式进行身份认证，对令牌设置合理的有效期和刷新策略，并在检测到异常活动时可以采取令牌失效等措施。前端在浏览器 localStorage 或 sessionStorage 中存储访问令牌等维持登录状态所必需的信息，但不会在客户端明文存储您的账户密码，我们也建议您在使用结束后及时退出登录并清理相关本地数据。

访问控制与最小权限原则

对涉及个人信息和业务数据的后台系统，我们实行账号分级与访问控制，仅授权为履行职责所必需的人员在相应权限范围内访问相关数据，并记录重要操作和访问行为日志，以便开展必要的安全审计和问题排查。

数据存储与备份保护

我们不设置登录密码，用户登录通过发送到您邮箱的一次性验证码完成。验证码仅用于短期身份验证和会话建立，不在系统中长期保存。为保护您的个人信息和业务数据，存放相关数据的服务器采取访问控制、系统加固和定期更新安全补丁等措施，以降低未授权访问、恶意攻击和数据泄露的风险。同时，我们会根据业务需要对关键数据实施定期备份，并对备份数据施加相应的访问限制和安全管理措施，防止备份数据被未授权访问、篡改或滥用。

安全监测与事件响应

我们通过访问日志、错误日志和异常行为检测机制等方式，对可能影响系统安全和稳定运行的行为进行监测，例如异常高频请求、异常登录尝试或疑似恶意抓取行为，并视情况采取限流、临时限制访问或封禁账号等措施。如发现存在或可能存在个人信息泄露、篡改或丢失等安全事件，我们将按照法律法规和相关监管要求启动应急响应，采取补救措施，并在需要时向您和有关主管机关告知相关情况。

您的安全责任

尽管我们已采取合理和必要的安全措施，但互联网环境下的信息传输和存储仍可能面临风险。您应当妥善保管账户及登录凭证，不向他人泄露，不在不受信任的设备或网络环境下长期保持登录状态。如您发现账户可能已经泄露，或出现异常登录、异常操作等情况，请及时通过本政策列明的联系方式与我们取得联系，我们将协助您采取相应保护措施。

十一、政策更新

我们可能不时更新本政策。若涉及重大变更，我们将更新“生效日期”并可能提供额外通知（如站内公告或邮件通知）。

继续使用本服务即视为您接受更新后的政策。

十二、联系我们

如对本政策有任何疑问，请联系我们：

同济大学杨龙课题组(https://www.yanglonggroup.com)

地址：中华人民共和国上海市嘉定区曹安公路 4800 号同济大学

邮箱：long_yang@tongji.edu.cn