Privacy Information

The research portal and repository Pure records and manages the research-relevant data of Technical University of Leoben. Furthermore, it connects competencies and serves as a scientific platform where researchers can present and manage their achievements, areas of expertise, and collaborations to strengthen the university's public profile.

The system is divided into two areas: the publicly visible portal (pure.unileoben.ac.at) and the web application (pureadmin.unileoben.ac.at/admin/workspace.xhtml), which serves as a personal workspace. Researchers manage their research output using the workspace, enter data, and control its visibility.

By law, the university is obligated to collect research achievements, but the quality of the data is the responsibility of the researcher.

To use the personal workspace in Pure, it is necessary to allow the processing of data. Otherwise, the system cannot be used. As the system operator, we take your right to data protection, privacy, and informational self-determination very seriously. You have the right to be informed, and we are happy to explain here what happens to your data.

The system operator aims to provide every user with a convenient, secure, and legally compliant access to the internet. The login method used is SAML2/Shibboleth via Keycloak or SSO.

What data is processed?

The system must recognize that you are authorized to access it. For internal Pure login, it is checked whether the entered password matches the username. If external authentication is chosen, e.g., SSO, an external instance verifies whether the username and password used have the appropriate authorization in that external instance.

The login data you enter, such as email address, username, and password, are stored locally on the system and partially matched with external databases and transmitted to them. This applies to login via SSO. These data are usually already known beforehand, for example, from an employee database. However, they never include special categories of data as defined in Article 9 of the GDPR, but only the identification necessary for the service provided to you.

User data includes username, first and last name, email address, role, and associated person. These are only visible in the workspace and not in the frontend.

Personal data consists of: first and last name, gender, date of birth, title, ID, employment relationship, organizational affiliation, start and end date at the institution.

Technical University of Leoben points out, in accordance with § 2d para. 1 Z 5 lit a FOG, that the processing of your personal data within the framework of research projects is lawful based on the Research Organization Act (Art. 6 para. c and Art. 9 para. g and j GDPR in conjunction with § 2d para. 2 FOG), and all necessary measures are adhered to.

What about cookies?

Only technically necessary cookies are used for the system's login page and are stored only for the duration of the session. On most mobile devices, these cookies are deleted immediately after a successful login. However, in some cases, this may depend on the individual settings of the browser used.

What are cookies?

Cookies are small text files created by a website during your visit. Most of them, called session cookies, are technically necessary for a browser session and are deleted when the browser is closed. Among other things, they enable the functionality of the browser's forward and back buttons. Some login methods do not work without them.

Are data shared with third parties?

For the processing of your personal data, we use Elsevier as a data processor, with whom we have taken sufficient guarantees to protect your personal data.

Beyond this, your data is not shared with third parties.

If your personal data is processed for research purposes, it is possible that these – in compliance with the requirements – may be transmitted to other research institutions as defined by the Research Organization Act. Furthermore, they may be subject to freedom of information regulations.

How are the data protected against unauthorized access?

In general, the system is a closed system with a high-security standard. It does not allow external processes to run on it, such as an app on a phone or a program on a laptop, thus eliminating common entry points for potential attackers. The default settings are data-minimizing, and the querying of sensitive data is not intended. All these measures make the system less attractive to attackers.

Access to stored data is regulated within the system through user management. The authorization management ensures that administrators are trained in data protection and handle data with due care in accordance with the GDPR. All accesses are password-protected, encrypted, and logged.

How long are the data stored?

User Data:

User data is used to access the workspace.

The user data (ID, first and last name, email address) is deleted after the termination of the employment relationship, usually 40 days after the end of the employment. Currently, an additional 30-day grace period is in place.

Personal Data:

Personal data is deleted upon the individual's request. Legal retention periods or the pursuit of potential legal claims may prevent deletion (Art. 17 para. 3 lit. d, e GDPR) and require longer retention.

The specific retention period of your personal data may vary depending on the research project. In general, personal data processed for the fulfillment of the university's tasks (e.g., scientific research and teaching) in the public interest for archival purposes related to scientific or historical research may be stored and further processed indefinitely (Art. 5 para. 1 lit. e GDPR, § 89 GDPR in conjunction with § 2d para. 5 FOG). Personal data lawfully collected by the university independently of a specific

research project may be reused for scientific research purposes. Further processing for another purpose is permissible under Art. 5 para. 1 lit. b GDPR.

Log & Audit Data:

The running system stores internal logs with IP addresses and usernames to ensure error-free operation. These logs are also only accessible to administrators and serve audit purposes.

Deletion generally occurs after 7 years for the content-related audit entries.

Your Rights

In general, you have the rights to access, rectification, data portability, restriction, deletion, withdrawal, and objection.

You can exercise your rights at the following address: dsb@unileoben.ac.at

If you believe that the processing of your personal data violates data protection law or your data protection rights have been infringed in any other way, you have the right to lodge a complaint with a supervisory authority.

In Austria, the competent authority is the Austrian Data Protection Authority.

Contact

Technical University of Leoben

Franz Josef-Straße 18

8700 Leoben

Email: dsb@unileoben.ac.at

If you have further technical questions, please contact: pure-admin@unileoben.ac.at

External Data Protection Officer

Stanonik Rechtsanwälte

Porzellangasse 37/13

A-1090 Wien

mul.datenschutz@stanonik.at