COLLECTING PERSONAL DATA: REPORTING REQUIREMENT IN ACCORDANCE TO GENERAL DATA PROTECTION REGULATIONS

When opening a JKU Partner Account

The Johannes Kepler University Linz (hereinafter referred to as the "JKU") would like to provide information about automatically processing your personal information (more precisely: personal information that can identify you) in accordance with Art. 4, para. 1 of the General Data Protection Regulations (hereinafter referred to as "GDPR") in which protection is governed by valid data protection[1] law. Under Art. 4 para. 2 of the GDPR, automated processing means collecting, recording and storing personal information by (automated) means.

I. Contact Information by the Responsible Party:

The Johannes Kepler University Linz (JKU), Altenberger Straße 69, 4040 Linz, datenschutz@jku.at, is responsible for processing the information described below under Art. 4 para. 7 of the GDPR

As stated in Art 37 of the GDPR, the designated Data Protection Officer is available at the Johannes Kepler University Linz (JKU), Office of Data Protection, Altenberger Straße 69, A-4040 Linz, Austria, datenschutz@jku.at.

II. Background for Processing / Indicating the Purpose for Collecting Personal Information / Legal Basis for Processing / Recipient for the Personal Information:

1. Background and Reasons for Processing

1.1. When creating a JKU Partner Account, the JKU will process your personal data (submitted either personally by you, or by an authorized person, such as your employer, for example), namely contact information and basic information, in particular the form of address, title [optional], first and last name, date of birth, address, e-mail address. and, if applicable, company data, in order to implement, administratively process, and manage various (user) authorization (such as access to IT systems, parking authorization, access to buildings/rooms), and the related legal relationship(s) with you, such as access to IT systems, parking authorization, access to buildings/rooms), and related legal relationship(s) with you by creating new users in the JKU IT system to access requested authorization(s), or to renew and extend

[1] Regulation (EU) 2016/679 by the European Parliament and of the Council on April 27, 2016 to protect individuals with regard to processing personal data, the free movement of this kind of data and repealing Directive 95/46/EC (**GDPR**); Federal Act to protect individuals with regard to processing Personal Data (DSG), BGBl. I No. 165/1999, as last amended by BGBl. I No. 14/2019; Directive (EU) 2016/680 by the European Parliament and the Council on June 27, 2016 to protect individuals with regard to processing personal data and the free movement of this kind of data (Directive). Directive (EU) 2016/680 by the European Parliament and the Council on April 27, 2016 to protect individuals with regard to processing personal data by the responsible authorities for the purposes of preventing, conveying, detecting or prosecution of criminal offences or enforcing sentences, on the free movement of this kind of data and repealing Council Framework Decision 2008/977/JHA (**Directive on data protection in the field of justice and domestic affairs**), implemented in Articles 36-61 DSG.

them, as well as to assert, exercise, or defend any legal claims and/or any investigation of criminal offenses or legal violations.

1.2. The JKU will also process your login information (log data) in relation to administration and processing (user) authorization by using and operating electronic access control systems and equipment (such as barrier systems in parking areas). The purpose is to guarantee and ensure regulated and authorized access to any (restricted) areas/spaces, premises, and buildings at the JKU, as well as to safeguard employees, buildings, rooms, property, and infrastructure at the JKU. We explicitly state that in accordance to Art. 9 GDPR, no biometric or other sensitive data will be processed as part of the electronic access control systems and facilities.

1.3. The JKU will also process your login data in order to maintain cost transparency to record and invoice expenses and fees when using electronic IT systems, such as the JKU telephone systems (billing and calling data, such as phone number/extension, number and call duration, call zones, billing period, total costs, etc.). Location or mobile data (local position) will not be processed.

1.4. In addition to the aforementioned reasons to process information, we may process your login data to safeguard system functions and security, analyze and correct any technical errors, and optimize system performance, meaning to the extent that this is technically necessary.

2. The Legal Basis

2.1. The legal basis to process personal data is to prepare a contract, or establish, fulfill and process a contractual relationship in accordance with **Art. 6 para. 1 lit. b GDPR** as well as the JKU's legitimate interest in accordance with **Art. 6 para. 1 lit. f GDPR** to properly (lawfully) process the application or account, manage the account's administration and process and/or (user) authorization(s), ensure adherence to the university's regulations and support security, protect property and personal protection, and ensure that the technical system functions flawlessly. The JKU's legitimate interests also include asserting, exercising and/or defending any legal claims and investigating criminal offenses or legal violations.

Processing data (meaning collecting, retaining, forwarding) is based on **Art. 6 para. 1 lit. c GDPR** to, if necessary, comply with any legal obligations, in particular legal obligations to which the JKU is subject to (see below).

2.2. The following applies to personal data you provide directly: If providing personal data for individual data processing is required by law and/or a contract, failure to provide this data may result in being unable to fulfill the above objectives; in particular, the requested JKU Partner Card account cannot be opened and processed.

3. Recipients

3.1. Those receiving the personal data include organizational departments at the JKU and their (required) auxiliary departments in order to process the application, in particular the Department of Facilities Management, Information Management, and the JKU institute/department involved in processing the application.

3.2. Processors involved in technical support, hosting, maintenance and administration, if they cannot be excluded from access to personal data by means of technical and organizational measures.

3.3. We may forward personal data to courts, authorities and/or legal representatives in order to assert, exercise or defend claims and investigate criminal offenses or legal violations. In addition, legal stipulations may require compliance with an obligation to collaborate with authorities, courts, and other authorities, constituting a legal basis to transfer or grant access to data (such as Section 46 (6) of the Austrian Universities Act, Section 76 StPO, Art 31 and 58 GDPR).

III. Retaining Personal Data:

Your personal data will be processed in accordance with any statutory retention and documentation periods. In addition, the retention period will be determined in accordance with the specified criteria relating to the retention period, such as timeliness and relevancy to the stated purpose(s), and any proof required to correctly conduct a legal relationship with you in the event of any disagreements or legal disputes.

We may store your personal data in order to preserve evidence, assert legal claims, and/or investigate criminal offenses and/or legal violations pending the legally binding outcome of official/judicial proceedings.

The access logs will be saved in the JKU's IT system for the aforementioned purposes for a period of seven days and then deleted. As outlined in the preceding paragraph, they may also be stored beyond this period, if necessary, to preserve evidence and enforce (any) legal claims, or investigate criminal offenses and legal violations in individual cases.

The telephone invoicing and call records will be retained for a six-month period and then deleted. In this regard, please also refer to the preceding paragraph.

IV. Data Subject Rights in accordance with Art. 15 - 21 GDPR:

- Right to access information
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

V. Information about the Data Protection Authority and the Data Subject's Right to Appeal:

In addition, the data subject may lodge a complaint to the Austrian Data Protection Authority, Barichgasse 40-42, 1030 Vienna, Ph.: + 43 1 52 152-0, E-mail: dsb@dsb.gv.at, if the data subject believes the procedure to process personal information relating to him or her infringes the regulations.

Last Update: January 2024