randevuUG(haftungsbeschränkt)
hello@randevu.tech ·
www.randevu.tech

randevu

Data Processing Agreement

This Data Processing Agreement (hereinafter: "DPA") is entered into between randevu UG randevu UG (haftungsbeschränkt), Samariterstraße 13, 10247 Berlin (HRB 231871 B) (hereinafter: randevu), and the Customer and forms an integral part of the Agreement. For the purpose of this DPA, the entity acting as randevu hereunder is the entity acting as randevu under the Agreement, as designated in accordance with the Section "Contracting Party, Governing Law and Venue" of the Agreement. randevu and the Customer hereinafter shall be recognized by the term "The Parties" or "randevu" or "the Customer".

The DPA is effective upon acceptance or signing of the Agreement or upon signing of this DPA by both Parties. It supplements, and does not supersede or cancel, the Agreement, which remains in full force and effect according to its terms. In the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will apply.

Regarding processing of Personal Data, this DPA and Appendix 1; 2 and 3 shall constitute the whole contractual relationship between randevu and the Costumer and shall be equally legally binding and enforceable.

Terms not otherwise defined herein, including but not limited to the terms "controller" "data subject", "Personal Data", "processing", "personal data breach" and "supervisory authority" shall have the meaning as set forth in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) hereinafter: "General Data Protection Regulation" or "GDPR".

The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the GDPR.

1. Definitions

Agreement means randevu's Terms of Service and the side letter(s) agreed between the parties, if any.

Applicable Law means all laws, rules and regulations applicable to each Party in its use of or provisioning of the software or any services, including but not limited to those applicable to the processing of Personal Data. For the avoidance of doubt, this means, exclusively, the GDPR and all national laws of EU member states for the processing of Personal Data.

Personal Service Data means any Personal Data that is part of Service Data and which randevu or randevu's Affiliates, employees or agents may process on behalf of Customer in providing the Software or any Services in accordance with this DPA. This may include the Personal Data of any of Customer's employees or end-customers which is submitted to and processed within the Software or the Services by Customer. For the avoidance of doubt, Personal Service Data does not include (i) the sign up information of Customer's employees, which may include Personal Data (such as email, name, password, job title, company, localization data) and (ii) Personal Data about visitors to the randevu Website (as further set for in the Privacy Policy).

Service Data means any information processed or transmitted by or on behalf of Customer in the Software or in connection with the performance of the Services during the Subscription. All Service Data processed under the terms of this Agreement will remain the property of Customer.

Sub-processor means a third-party subcontractor engaged by randevu that performs randevu's obligations under this DPA on behalf of randevu. A list of current Sub-processors can be found in Appendix 3.

2. Scope of the DPA and roles of the Parties

2.1. This DPA shall apply to all processing activities of the personal data obtained in connection with or in regard with the usage of the Randevu Software or services, or in relation to any written or oral instruction of the Customer as a controller. Unless provided for otherwise in the Agreement, the processing will be limited to the storage or processing of certain limited Personal Service Data on a server and incidental access to such data when providing the Software or the Services pursuant to the Agreement. This DPA details the Parties' obligations in relation to the protection of Personal Service Data.

2.2. Customer shall be the "controller" in accordance with Art. 4.7 GDPR and randevu shall be "processor" in accordance with Art. 4.8 GDPR.

3. Nature and Purpose, Duration and Specification of Processing Operations

3.1. The nature and purpose of the data processing under this DPA is the provision of the Services and providing the Software and/or the Services to Customer and the performance of randevu's obligations under the Agreement and this DPA (or as otherwise agreed by the Parties).

3.2. The categories of Personal Data and data subjects which may be subject to the processing within the scope of this DPA are listed in Appendix 1. Appendix 1 is subject to change upon mutual acceptance by the Parties in written form.

3.3. The duration of the processing shall correspond to the Agreement Term. Customer as a data controller shall be obliged to determine the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. Customer as a data controller therefor shall be obliged to notify Randevu regarding the period for which the subject matter personal data is being stored.

4. Responsibilities

4.1. Within the scope of this DPA, Customer shall be solely responsible for compliance with Applicable Laws including but not limited to the lawfulness of disclosing

Personal Data to randevu and the lawfulness of having Personal Data processed on behalf of Customer.

4.2. Customer's individual instructions on data processing shall, initially, be as detailed in the Agreement. Customer shall subsequently be entitled to modify, amend or replace such individual instructions in writing or in a machine-readable format (e.g. via email) by issuing such instructions to the point of contact designated by randevu. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the Agreement.

Customer shall, without undue delay, confirm in writing or by email any oral instruction given.

5. randevu´s obligations

5.1. Except where expressly permitted by Art. 28 para. 3 lit. a) GDPR, randevu shall process Personal Service Data only within the scope of the Agreement and the documented instructions issued by Customer, unless required to do so by Applicable Law to which randevu is subject to. In such a case, randevu shall inform Customer of that legal requirement before processing, unless Applicable Law prohibits such information from being shared on important grounds of public interest. The aforesaid provisions shall also apply to the transfer of personal data to a third country or an international organization.

5.2. If randevu believes that an instruction would be in breach of Applicable Law, randevu will notify Customer of such belief without undue delay. randevu is entitled to not perform the relevant instruction until Customer confirms that it complies with Applicable Law or modifies such instruction. If certain data processing activities infringed the legally binding rules, whether determined by GDPR or other Applicable Laws, randevu shall have right to cease the processing until the Parties or competent authority provide evidence that such processing is compliant with the GDPR and other Applicable Law. Such undertakings of Randevu shall not be considered as a breach of its contractual obligations under this DPA.

5.3. If certain data processing activities infringed the legally binding rules, whether determined by GDPR or other Applicable Laws, randevu shall have right to cease the processing until the Parties or competent authority provide evidence that such processing is compliant with the GDPR and Applicable Law. Such undertakings of randevu shall not be considered as a breach of its contractual obligations under this DPA.

5.4. randevu shall, within randevu's scope of responsibility, put in place appropriate safeguards and security measures so that it satisfies the specific requirements of the Applicable Law. randevu shall, in particular, taking into account the nature of the Personal Service Data and the risks involved in the processing of any such Personal Service Data, maintain reasonable and appropriate technical and organizational measures designed to ensure the adequate protection of Customer's Personal Service Data, which will fulfill the requirements of the GDPR and specifically its obligations under Art. 32 GDPR. The measures implemented at the time of establishing this DPA are set forth in Annex 2 to this DPA. Customer is familiar with these technical and organizational measures, and is responsible for determining that such measures ensure a level of security appropriate to the risk associated with Personal Service Data. randevu reserves the right to modify the measures and safeguards implemented, provided that the level of security shall not be less protective than initially agreed.

5.5. randevu shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk according to Art. 32 para 1 lit. d) GDPR, for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to reasonably ensure the security of the processing. randevu will further, by way of regular self-audits, reasonably ensure that the processing of Personal Service Data conforms with the above-mentioned provision according to Customer's instructions or as agreed with Customer.

5.6. Taking into account the nature of the processing, randevu shall implement appropriate technical and organizational measures, insofar as this is possible, in order to assist Customer to fulfil the Customer's obligation to respond to requests for exercising data subjects' requests, as laid down in chapter III of the GDPR. randevu shall assist Customer in ensuring compliance with the obligations pursuant to Art. 32 to 36 GDPR taking into account the nature of the processing and the information available to randevu.

5.7. randevu ensures that (i) any person authorized to process Personal Service Data on behalf of the processor have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. All employees authorized to process Personal Service Data and other such persons as may be involved in data processing within randevu's scope of responsibility is prohibited from processing Personal Service Data outside the scope of the instructions, unless required to do so by Applicable Law.

5.8. randevu shall notify Customer, without undue delay, if randevu becomes aware of a personal data breach within randevu's scope of responsibility. In the event of any breach, randevu shall implement the measures necessary to secure Personal Service Data and mitigate potential negative consequences for the affected data subjects. randevu shall coordinate such efforts with Customer without undue delay. randevu shall notify Customer of the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

5.9. randevu shall correct or erase Personal Service Data if so, instructed by Customer and where covered by the scope of the instructions if this is permissible. Where an erasure consistent with data protection requirements or a corresponding restriction of processing is impossible, randevu will, based on Customer's instructions, and unless otherwise agreed in the Agreement or legally binding rules, destroy all carrier media and other material or return the same to Customer in compliance with data protection requirements. In specific cases designated by Customer, such Personal Service Data will be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

5.10 randevu shall, upon termination of the data processing and upon Customer's instruction, return all Personal Service Data, carrier media and other materials to Customer or delete the same. In case of testing and discarded material, no instruction shall be required.

5.11. Where a data subject asserts any claims against Customer in accordance with Art. 82 GDPR, randevu will support Customer in defending against such claims to the extent they arise in connection with the processing of Personal Service Data by randevu within the scope of this DPA only, and to the extent this is possible. Provided that such claims are not based on randevu's breach of duties, randevu reserves the right to a reasonable compensation for such support.

6. Customer's obligations

6.1. Customer shall notify randevu in sufficient detail and without undue delay of any defect or irregularity detected by Customer in randevu's provision of the Software or the Services concerning data protection.

6.2. Section 5.11 of this DPA shall apply, mutatis mutandis, to claims asserted by data subjects against randevu in accordance with Art. 82 GDPR.

6.3. Customer shall notify randevu's point of contact for any issues related to data protection arising out of or in connection with the Agreement.

6.4. Customer shall notify randevu in writing of the names of the persons who are entitled to issue instructions to randevu. Unless otherwise specified at a later date, the point of contact designated in the Agreement or during the onboarding process shall be entitled to issue instructions. If no point of contact has been designated, the managing directors of the Customer shall be entitled to issue instructions to randevu. Randevu shall immediately inform the Customer if, in its opinion, an instruction infringes Applicable Law.

7. Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure (deletion), restriction (blocking), transmission or access against randevu, and where randevu is able to correlate the data subject to Customer based on the information provided by the data subject, randevu shall refer such data subject to Customer. randevu shall forward the data subject's claim to Customer without undue delay. randevu shall support Customer, to a reasonable extent and based upon Customer's instructions. randevu shall not be liable in cases where Customer fails to respond to the data subject's request or fails to do so correctly and/or in a timely manner.

8. Options for documentation and audits

8.1. randevu shall document and make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA. Customer shall have the right to assess randevu's compliance with the obligations agreed upon in this DPA by appropriate measures.

8.2. In addition, randevu allows for and contributes to audits, including inspections, conducted by Customer or another auditor mandated by Customer or a supervisory authority. In particular, randevu agrees that Customer or an auditor mandated by Customer is entitled, after giving reasonable advance notice (usually no less than ten (10) calendar days), to on-site check the compliance with the provisions on data protection and the contractual agreements of this DPA provided that such on-site inspections will be conducted to the extent necessary outside normal business hours of randevu (e.g. on the weekend and in evening on working days) and without disrupting randevu's operations; it is understood that such audits include obtaining of information and inspection of the personal data stored. randevu shall be entitled to reject auditors that are competitors of randevu. At least one employee of randevu may accompany the auditors at any time. randevu may memorialize the results of the audit in writing which shall be confirmed by Customer.

8.3. randevu may also determine that any audits and inspections require the execution of a usual and mutual confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organizational measures and safeguards implemented. In this case, execution of such a confidentiality undertaking will be a prerequisite for any audit or inspection.

8.4. randevu's time and effort for such inspections shall be limited to, unless agreed upon otherwise or determined by Applicable Law. randevu reserves the right to charge a reasonable fee for randevu's support in conducting inspections, to the extent such support exceeds one working day (8 hours) per calendar year, based on randevu's reasonable costs.

8.5. When a supervisory authority undertakes inspection within the processor, the processor shall be obliged to comply in accordance to the provision of the Chapter 6 of the GDPR and other Applicable Law.

8.6. randevu shall audit its Sub-processors (as defined below) on a regular basis and will upon Customer's request confirm their compliance with Applicable Law and the obligations set upon the Sub-processors according to the data processing agreement concluded with them while randevu is obliged to implement at minimum the same compliance criteria with its sub-processor as it has been determined within this DPA.

9. Sub-processor

9.1. Customer herewith authorizes randevu in general to engage sub-processors. randevu shall conclude with such Sub-processors data protection obligations enabling the same level of data protection and information security in accordance with Art. 28 para. 4 GDPR and the provisions of this DPA. Where randevu commissions Sub-processors, randevu is responsible for ensuring that every Sub-processor is subject to obligations regarding the processing of Personal Data that are no less protective than those to which randevu is subject under this DPA.

9.2. If randevu intends to assign a new sub-processor or to replace an existing sub-processor, randevu shall be obliged to notify and justify its need for assignment of another sub-processors to the Costumer. Upon the notification of randevu, the Constumer, whitin 30 calendar days, shall have right to object to such other sub-processor on the grounds of sub-processor's failure to meet safeguard and security measures determined by this DPA, the GDPR and the member states applicable laws. The Customer shall not have right to object another sub-processor on its merit, reputation nor any other ground but data protection requirements. If the Customer abuses right to object, randevu shall have right to terminate this DPA and the related Agreement without obligation to refund insofar withhold fees.

9.3. If Customer does not object to the engagement of a third party in accordance with this Section within 30 calendar days after notice is given by randevu, the Sub-processor shall be deemed a Sub-processor to which Customer consented for the purposes of this DPA. In the event, Customer does not agree to the engagement of such sub-processor, both parties will use reasonable efforts to find an amendment in the Agreement to avoid processing of Personal Service Data by the objected-to sub-processor. If the parties are unable to find a mutually acceptable solution during the aforementioned 30 days time limit, the parties may, in their reasonable discretion, terminate the Agreement extraordinarily.

9.4. randevu is entitled to engage a Sub-processor located outside the EEA, the United Kingdom and Switzerland upon prior written approval of the Customer and after amending the appendix 3 of this DPA. If so, randevu shall implement appropriate contractual and technical safeguards to ensure compliance with the requirements in accordance to the applicable requirements set out within the Chapter 5 of the GDPR on the transfers of personal data to third countries or international organizations. For compliance with the transfers of personal data to third countries or international organizations, randevu shall enter into contractual obligations which ensures compliance with the Chapter 5 of the GDPR. randevu may amend or replace the SCC by other appropriate safeguards as required under Applicable Law for transfers of Personal Data to third countries once made available by the European Commission or once further guidance about the use of the SCC and accompanying supplementary measures becomes available. randevu will conduct a transfer impact assessment prior to the engagement of any new Sub-processor located outside the EEA, the United Kingdom and Switzerland.

10. SCC

If Customer is a Controller located outside the EEA, enters into this Agreement including a DPA with randevu UG, and chooses a data location within the EEA, randevu and Customer hereby agree that Module 4) of the SCC (Controller to Processor) apply and randevu shall be acting a Data Exporter and Customer acting as Data Importer within the meaning of the SCC.

11. Safeguards and Support for international data transfers

randevu undertakes to provide reasonable support to Customer to ensure compliance with the requirements imposed on the transfer of Personal Data to third countries with respect to data subjects located in the EEA, United Kingdom and Switzerland. randevu will do so, in particular, by providing information to Customer which is reasonably necessary for Customer to complete a Transfer Impact Assessment (hereinafter TIA). Customer warrants that it will have successfully completed an appropriate TIA prior to any processing under the DPA if required.

12. Liability and damages

The provisions on the Parties' liability contained in the Agreement shall apply to any liability relating to data processing, unless otherwise agreed in this DPA.

13. Modifications

The Parties may modify or supplement this DPA, with notice to the other Party, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Art 40, 42 and 43 of the GDPR. The informed Party shall notify the modifying Party if it does not agree to a modification, in which case the informed Party may terminate this DPA and the Agreement with two (2) weeks' prior written notice. Customer shall not be entitled to any refund of Fees unless the objection to the modifications are based on justified reasons of non-compliance with Applicable Law, in which case it is entitled to receive a pro-rata refund of any Fees paid.

14. Obligations to inform, mandatory written form, choice of law

Where the Personal Service Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by Third Parties while in randevu's control, randevu shall notify Customer of such action without undue delay.

No modification of this DPA and/or any of its components shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this DPA. The foregoing shall also apply to any waiver or modification of this mandatory written or text form. Notwithstanding the form of modification of this DPA, both Parties shall accept the modification in the way determined by governing law or by mutual agreement of the Parties, which includes but not limited to signing the modification or expressly accept it by using word such as "accept" or similar.

In case of any conflict, the data protection regulations which includes the GDPR and other Applicable Laws shall take precedence over the provisions of the Agreement. Should any provision of this DPA be held or declared invalid, unlawful or unenforceable the remaining provisions shall remain valid.

This DPA is governed by the laws of the Federal Republic of Germany and the place of jurisdiction shall be Berlin unless and to the extent required otherwise by applicable data protection and privacy laws.

02.06.2003. Berlin
Date, Place

Aleksandar Orlic
Signature/First name, Last name
randevu UG (haftungsbeschränkt)

01.06.2023 Walldorf
Date, Place

Matthias Döpke
Signature/First name, Last name
The Customer (iX3 GmbH)

Appendix 1 – Specifications of the Processing

1. Types of personal data

The processor shall process on behalf of the controller the following personal data: basic and other informational personal data (names, emails, payment information, profession, etc) of our users in the system and meta data created in stored in data structures known to our customers (i.e. data containing information on characteristics of other data) and purchase data.

2. Categories of data subjects

Personal Data being processed by randevu on behalf of Customer could refer to any category of data subject that Customers provide in randevu tech platform including but not limited to Customer's customers and potential customers, employees, suppliers and other Customer contacts.

Appendix 2 -. Technical and Organizational Measures

1. Confidentiality, Integrity, Availability and Resilience (Art. 32 para. 1 lit. a) GDPR; Art. 25 para. 1 GDPR)
   a. Confidentiality (Art. 32 para. 1 lit. b) GDPR)
      i. Physical Access Control (Measures to prevent unauthorised access to data processing equipment with which Personal Service Data may be processed and used):
         - randevu Platform SaaS is hosted at an external cloud service provider (see the Appendix 3), with whom randevu has a data processing agreement in place.
         - Randevu does not operate any own physical data storage for personal data
      ii. Electronic Access Control (Measures to prevent unauthorized use of data processing systems):
         - Access is secured via a firewall, with strong encryption and by two-factor authentication mechanisms.
         - Secure passwords are stored in encrypted form. Their structure and handling is in accordance with a documented password guideline.
         - An effective and documented access control policy exists.
         - The access control policy is assessed at least once per year.
         - All staff are instructed to lock their workplaces when they leave them. Workplaces are configured with an automatic lock as standard.
      iii. Internal Access Control (Measures ensuring that authorized persons only have access to the Personal Service Data covered by their access authorization, and that prevent unauthorized reading, alteration or erasure during processing, use and storage):
         - Release of Personal Service Data only to authorized persons, including allocation of differentiated access rights and roles.

- Access rights are adjusted if the tasks carried out in the business processes change and/or are withdrawn if they are no longer needed.

b. Integrity (Art. 32 para. 1 lit. b) GDPR)

i. Data Transfer Control (Measures that prevent unauthorized reading, alteration or erasure during processing, use and storage of Personal Service Data during electronic transfer, storage on data media or during transportation):

- Use of adequate encryption technologies for passwords and other sensitive information
- Using not structured storage for meta data
- No physical transport of the Personal Service Data (e.g. via data carriers)
- Use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the Personal Service Data travels. It is handled through external cloud service provider (see the Appendix 3)

ii. Data Entry Control (Measures that are suited to verify whether any by whom Personal Service Data been entered into, altered in or removed from data processing systems):

- Plausibility is guaranteed via the Login functions of the randevu Platform SaaS.
- Log systems and logging information are protected against unauthorised access, alteration and erasure, and are regularly evaluated.

iii. Order Control (Measures that are suited for ensuring that the commissioned processing of personal data complies with the guidelines of the contracting Party):

- randevu has data processing agreements with the sub-processors who process Personal Service Data on randevu's behalf in place.

- External service-providers are evaluated before being contracted.

iv. Separation rule (Measures that are suited for ensuring that data that has been collected for different purposes can be kept separate during processing):
- Meta data is handled separately of the real data it describes
- Access to Personal Service Data is separated through application security for the appropriate Customers.
- Personal Service Data that have been collected for different purposes are kept apart in such a way (physically or logically) that they are separated, processed, stored and erased in a manner appropriate to the purpose.
- Development, testing and production environments are separated.

c. Availability and Resilience (Art. 32 para. 1 lit. b) GDPR) (Measures to prevent accidental or willful destruction or loss):

i. All Personal Service Data processed by randevu Platform Saas is stored on servers from our Cloud Service Provider (see Appendix 3) and randevu offers same levels of service

d. Incident-response-management (Measures suited to ensure that data breaches are recognised and reported quickly):

i. A process has been established which ensures that security incidents are identified, assessed and dealt with appropriately.

ii. Escalation procedures and organisational interfaces are defined with all relevant parties.

iii. Staff who are responsible for the management of IT systems/applications are trained to recognise, classify and report security incidents.

iv. A process has been established which ensures information security for all critical business processes, even during a crisis or catastrophe.

   v. Processes and responsibilities have been defined in case of an emergency or crisis.

e. Regular testing, assessment and evaluation processes (Art. 32 Paragraph 1 Point d) GDPR) (Measures guaranteeing that the data protection requirements are implemented):

   i. Relevant staff are trained and familiarised with data protection and placed under an appropriate obligation.

   ii. The IT operation procedures (e.g. user management, backup, network management) are comprehensibly documented, regularly checked and altered where necessary.

   iii. Identification, provision and testing of updates are a part of standard operation.

      - Regulations exist for information security and data protection.

   iv. The regulations for information security and data protection, as well as the security measures, are tested regularly for compliance and effectiveness.

Appendix 3 - randevu Sub-processors

Sub-processors processing Personal Data Personal Service Data uploaded by Customer or its Customers to the randevu Platform SaaS Offerings.

Sub-processor	**Purpose**	**Location (by country)**
AWS	randevu Platform SaaS Infrastructure	Germany