randevu GmbH
Samariterstrasse 13
10247 Berlin

DATA PROCESSING AGREEMENT

This Date Processing Agreement "DPA" is entered into by the Parties set out below in connection with the Agreement between the Customer and randevu, including the Terms of Use of randevu. This DPA forms an integral and inseparable part of the Agreement.

1. PARTIES TO THIS DPA

A) The customer party to the Agreement, defined in the Terms of Use as You (herein "**Customer**")
B) randevu GmbH (“**randevu”**)
Samariterstrasse 13, 10247 Berlin, Germany
Registration Number HRB 231871 B

The Customer and randevu are hereinafter jointly referred to as the "Parties" and each separately as a "Party".

This DPA has been pre-signed on behalf of randevu and shall become effective when electronically agreed to by the Customer. The Customer represents to randevu that the person agreeing has the legal authority to agree to and enter into this DPA.

2. BACKGROUND AND CONFLICT RULES

This DPA sets out the terms and conditions for the processing of Personal Data by randevu on behalf of the Customer under the Agreement for the purpose of providing the Service to the Customer. This DPA includes Standard Contractual Clauses ("SCCs") attached hereto as Appendix 1.

In the event of any discrepancy between this DPA and the Terms of Service, this DPA prevails, in case of any discrepancy between this DPA and the SCCs, the SCCs prevail, and in case of any discrepancy between the Terms of Service and the SCCs, the SCCs prevail.

3. DEFINITIONS

Unless otherwise defined in this DPA, terms used in this DPA, such as "Data Controller", "Data Processor" and "Data Subject" have the meanings as defined in the Data Protection Regulation.

randevu GmbH
Samariterstrasse 13
10247 Berlin

A) **Data Protection Regulation** means all applicable laws relating to data protection, including without limitation the laws implementing EU Directive 95/46/EC and EU Directive 2002/58/EC and the GDPR (when applicable) and any amendments to or replacements for such laws and regulations.
B) **GDPR** means the General Data Protection Regulation (EU) 2016/679.
C) **Personal Data** means any information relating to an identified or identifiable natural person, and which randevu has received from the Customer under the Agreement.
D) **Personal Data Breach** means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by randevu on behalf of the Customer.
E) **Standard Contractual Clauses** ("SCCs") means the contractual clauses issued by the European Commission by the decision 2010/87/EU for international transfers of Personal Data.
F) **Website** means randevu's internet website at https://randevu.tech.

4. PROCESSING OF PERSONAL DATA

To the extent the Customer inputs Personal Data into the Service and randevu processes such Personal Data, the Parties acknowledge that the Customer acts as Data Controller and randevu is the Data Processor processing Personal Data on behalf of the Customer.

Processing of Personal Data under this DPA is for the purpose of providing the Service to the customer. Processing of Personal Data in this context refers mainly to maintenance, storage, technical support and other equivalent processing activities. The categories of Data Subjects processed for the purposes of the Service include Customer's representatives and end-users. Type of Personal Data processed contains information, including Personal Data, uploaded to the Service by the Customer or its end-users, for example contact details and purchase data.

Personal Data may be processed as long as the Service is provided under the Agreement and after that if required by applicable law or contractual obligations or rights of either Party.

5. CUSTOMER'S INSTRUCTIONS

randevu shall process Personal Data in accordance with the Customer's written instructions as established in this DPA. The Parties agree that this DPA is the Customer's complete written instruction to randevu in the Customer's role as the Data Controller. Additional instructions require prior written agreement between the Parties.

randevu GmbH
Samariterstrasse 13
10247 Berlin

6. RANDEVU'S GENERAL OBLIGATIONS

randevu shall process Personal Data in compliance with Data Protection Regulation and on written instructions from the Customer, unless prescribed otherwise by a provision of Data Protection Regulation applicable to randevu.

randevu shall ensure that randevu's staff with access to Personal Data has committed to appropriate confidentiality.

randevu shall, at the Customer's written request, provide reasonable assistance to the Customer by providing such readily available information, or creating such information, as the Customer may reasonably require and which the Customer does not have, in complying with the requests of the Data Subject or supervisory authority or any other law enforcement or regulatory authority. randevu shall provide reasonable assistance to the Customer in ensuring compliance with its obligations set out in Data Protection Regulation. randevu is entitled to charge the Customer for costs and expenses that were incurred as a result of such assistance.

randevu shall inform the Customer, as soon as reasonably practicable, if it receives a request from a Data Subject seeking to exercise his or her rights under the Data Protection Regulation.

randevu shall maintain records of processing activities under its responsibility to ensure randevu's own compliance as a Data Processor, to the extent necessary to demonstrate compliance with randevu’s obligations set out in this DPA and in the Data Protection Regulation.

7. DATA SECURITY

randevu shall implement and maintain appropriate technical and organisational measures to ensure an appropriate level of security of the Personal Data and to protect the Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure for the purposes of the Service.

In the event of a Personal Data Breach, randevu shall notify the Customer without undue delay after becoming aware of the Personal Data Breach and take reasonable steps to mitigate any damage resulting from such breach. The notification shall contain information randevu is reasonably able to disclose to the Customer, including the following information:

A. a description of the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned;
B. the name and contact details of contact point where more information can be obtained;
C. a description of the likely consequences of the Personal Data Breach; and

D. a description of the measures taken or proposed to be taken to address the Personal Data Breach.

The information may be provided in phases if it is not possible to provide the information at the same time.

randevu shall cooperate with and assist the Customer, at the Customer's written request and the Customer's cost and expense, in relation to the Personal Data Breach notifications made to supervisory authority as required under the Data Protection Regulation.

8. SUBCONTRACTORS

randevu is entitled to use subcontractors for the purposes of providing the Service under the Agreement. The Customer hereby consents to randevu's use of subcontractors as described in this section.

randevu shall use its commercially reasonable efforts to reasonably ensure that its subcontractors are subject to equivalent requirements regarding confidentiality and data protection, as set out in this DPA. randevu remains responsible for its subcontractors and their compliance with the obligations of this DPA.

9. TRANSFERS OF PERSONAL DATA

Personal Data shall be processed outside of the European Economic Area by randevu or its subcontractor.

If necessary, the Customer authorizes randevu to enter into a data transfer agreement with its subcontractors incorporating SCCs in the name and on behalf of the Customer. Notwithstanding the foregoing, the SCCs will not apply if randevu or its subcontractor has adopted alternative safeguards in accordance with the Data Protection Regulation for the lawful transfer of Personal Data outside the EEA, such as Privacy Shield.

10. AUDITING

At the Customer's written request, randevu shall provide the Customer with an audit report, which is not older than 12 months so that the Customer can reasonably verify randevu's compliance with its obligations under this DPA.

randevu GmbH
Samariterstrasse 13
10247 Berlin

The report shall at all times be deemed as randevu's confidential information.

11. . TERM AND TERMINATION

The DPA shall continue in force until the termination of the Agreement. Upon termination of the Agreement or upon the Customer’s written request, randevu shall either destroy or return to the Customer or a third party designated by the Customer in writing the Personal Data processed hereunder. If not instructed otherwise in writing by the Customer, randevu shall have the right to delete and destroy the Personal Data processed hereunder within three (3) months' of the termination of the Agreement. In case the Customer demands that the Personal Data are returned to the Customer or to a third party, the Customer will pay randevu for reasonable costs and expenses arising out such return of the Personal Data.

randevu GmbH
Samariterstrasse 13
10247 Berlin

APPENDIX 1
Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

the Customer, as defined in the Agreement (the data exporter)

and

randevu GmbH (the data importer)
Samariterstrasse 13, 10247 Berlin, Germany
Registration Number HRB 231871 B

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' must have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];
b) 'the data exporter' means the controller who transfers the personal data;
c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they consid-ered it better for the contract to stand alone.

randevu GmbH
Samariterstrasse 13
10247 Berlin

e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor must be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e) that it will ensure compliance with the security measures;
f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
j) j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer[2]

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory require-ments which do not go beyond what is necessary in a

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
d) that it will promptly notify the data exporter about:
    i. any legally binding request for disclosure of personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
    ii. any accidental or unauthorised access, and
    iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which must be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which must be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

---

democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

randevu GmbH
Samariterstrasse 13
10247 Berlin

Clause 6
Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of operation of law, in which case the data subject can enforce its rights against such entity.
   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor must be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer must promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter must be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses must be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer must not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under Clauses, with the consent of the data exporter, it must do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer must remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor must also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor must be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 must be governed by the law of the Member State in which the data exporter is established.
4. The data exporter must keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which must be updated at least once a year. The list must be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that upon the termination of the provision of data processing services, the data importer and the subprocessor must, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or must destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

randevu GmbH
Samariterstrasse 13
10247 Berlin

APPENDIX 1
to the Standard Contractual Clauses

This Appendix forms a part of the Standard Contractual Clauses.

Data exporter
The data exporter is the Customer defined in the Order and in the DPA, i.e. who creates an online marketplace that allows users to register accounts and store Personal Data.

Data importer
The data importer is randevu GmbH (the data importer), Registration Number HRB 231871 B, company incorporated and existing under the laws of Germany, having its principal place of business at Samariterstrasse 13, 10247 Berlin, Germany. randevu is the provider of Services.

Data Subject
Data Subjects include the data exporter's contact persons, customers and end-users.

Categories of data
The Personal Data relating to individuals which is uploaded into the Services provided by the data exporter. This Personal Data includes contact details, authentication data, transactional data and purchase data.

Special categories of data (if appropriate)
The Parties do not anticipate the transfer of special categories of data.

Processing operations
Personal Data is processed for the purpose of providing the Services which may include following processing activities:

i. maintenance, storage and prevention and detection of security issues;
ii. technical support and responses to customer requests; and
iii. other processing activities for the purpose of fulfilling the obligations under the Agreement.

Personal Data may be processed as long as the Services are provided under the Agreement and after the expiry or termination of the Agreement as long as required by applicable law or contractual obligations or rights of either Party.

randevu GmbH
Samariterstrasse 13
10247 Berlin

APPENDIX 2
to the Standard Contractual Clauses

This Appendix forms a part of the Standard Contractual Clauses.

randevu currently observes the security practices described in this Appendix. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, randevu may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. These security measures include:

Access control
randevu has appropriate technical and organizational measures in place to control access to systems and servers and to protect against unauthorized access. randevu maintains security measures to ensure that employees and subcontractors only have access to data they are authorized to process. This includes differentiated access rights, automated and manual software locking and mandatory change of default passwords and encryption of data.

Disclosure of data
Appropriate technical and organizational measures are taken to ensure that personal data cannot be read, copied, modified or removed in electronic transmission or during transport or storage of personal data. Aspects of the disclosure of personal data are controlled. Measures may include encrypted protocols of data transfers, tunneling (VPN) and data pseudonymisation whenever possible.

Input control
randevu has appropriate technical and organizational measures in place to verify and establish retrospectively whether and by whom personal data is processed. Modifications and deletion of data are logged and systems alert appropriate employees of malicious, unintended or anomalous activities.

Job control
randevu hosts its Services with trusted third party service providers. randevu relies on appropriate contractual arrangements, privacy policies and security policies to assure the protection of data processed or stored by these third party service providers.

Availability control
Appropriate technical and organizational measures are taken to ensure that personal data are protected against accidental destruction or loss. Measures include backup and incident management procedures and regularly tested data recovery.

Segregation control
Appropriate technical and organizational measures are taken to ensure that data collected for different purposes is processed and stored separately, i.e. segregation of clients and functions (production/testing).