Data Processing Agreement (DPA)

Data protection agreement (hereinafter referred to as contract) concerning the processing of personal data in the order (order processing according to Art. 28 GDPR)

The following translation is solely for your information. In the case of a conflict or discrepancy between the German version and this translation (including as a consequence of a delay in the translation), the German version shall prevail.

CLIENT

CONTRACTOR

RaiseNow AG
Hardturmstrasse 101
8005 Zürich, Schweiz

0. Scope and Subject Matter of this Contract

The Data protection agreement (hereafter referred to as contract) apply to the use of the IT and on and offline fundraising infrastructure available for purchase through www.raisenow.com and to any affiliated websites, digital services, browser plugins or applications, as well as to the underlying software (together the "Services") operated by RaiseNow AG, a company incorporated under Swiss law ("RaiseNow").

By signing the Individual Contract, the Customer expressly acknowledges this contract. If Customer does not agree to this contract, the Customer will not be able to access the Services.

Definition

As far as they are not defined otherwise in this document, all terms have the same meaning as in the Swiss Federal Act on Data Protection (“FADP”)and the EU General Data Protection Regulation (“GDPR”). This Contract is read and interpreted in the light of the provisions of the FADP and the GDPR, as applicable (“Data Protection Acts”). Clauses in this contract cannot be interpreted in a way that conflicts with rights and obligations provided for in Data Protection Acts, as applicable, or prejudices the fundamental rights or freedom of the data subjects.

1. Subject and term of the Agreement

The operational processing of personal data within the context of service provision is the service that is commissioned.

Processor will process personal data for the Controller within the meaning of Data Protection Acts on the basis of this Agreement.
The contracted service will be provided exclusively in a member state of the European Union or the European Economic Area. Any transfer of the service or partial work to a third country requires the prior consent of the Controller and may only take place if the special requirements of Data Protection Acts are fulfilled (adequacy decision by the Commission, standard data protection clauses, approved codes of conduct, etc.).

The contract period is based on the main contract.

2. Purpose, extent and nature of the processing, type of personal data and categories of data

1. In processing the data on order, the Contractor may not arbitrarily correct, delete or limit the processing thereof, but only upon documented instruction by the Client. If an affected person approaches the Contractor in this regard, the Contractor shall forward this request promptly to the Client.

2. Inasmuch as they are comprised in the scope of services, the concepts of deletion, right to be forgotten, correction, data portability and disclosure are to be ensured immediately in accordance with documented instruction of the Client.

3. Rights and obligations as well as instructions of Controller

Controller alone is responsible for assessing the admissibility of processing in accordance with Data Protection Acts as well as for protecting the rights of data subjects in accordance with Data Protection Acts. Nevertheless, Processor must forward all such inquiries, provided that they are identifiably directed exclusively to Controller, immediately to Controller.
Changes to the processed data and procedural changes must be set down in writing or in a documented electronic format.
Generally, the Controller will issue all processing requests, partial requests and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.
Controller has the right, as stated in number 5 above, prior to the start of the processing and thereafter on a regular basis, to verify the compliance of the technical and organizational measures taken by Processor as well as Processor's compliance with the obligations specified in this Agreement.

The Controller must inform the Processor immediately if it detects any errors or irregularities in verifying the results of the processing.
The Controller must handle with confidentiality all knowledge of Processor's business secrets and data security measures obtained as part of the contractual relationship. This obligation remains valid even after termination of this Agreement.

4. Controller employees authorized to give instructions and Processor employees authorized to receive instructions

Functions of the client authorized to issue instructions are specified in the main contract.

Communication channels to be used for giving instructions is by email to the following address: datenschutz@raisenow.com

In the event of a change in or long-term unavailability of a point of contact, the parties must notify each other immediately and in writing or electronically of the replacement or alternate point of contact. Instructions are to be kept on file for the remainder of their validity and thereafter for three full calendar years.

5. Obligations of Processor

Processor must process personal data only in accordance with prior arrangements and the instructions of Controller, unless required to otherwise process the data by Switzerland, the European Union or EU Member State law to which Processor is subject (such as investigations by law enforcement or national security agencies); in such a case, Processor must inform the Controller of these legal requirements prior to processing the data, unless the relevant law prohibits such information on important grounds of public interest (Article 28 (3) sentence 2 (a) GDPR).
Processor may not use the personal data provided for processing for any other purpose, particularly for its own purposes. Copies or duplicates of the personal data must not be created without Controller's knowledge.

Processor must cooperate to the extent necessary and adequately assist Controller as much as possible in fulfilling the rights of the data subjects per Data Protection Acts, preparing directories of processing activities and conducting the required data protection impact assessments (Article 28 (3) sentence 2 (e) and (f) GDPR). Processor must forward all information required for these purposes immediately to the authorized instruction giver named in section 4

Processor must notify Controller immediately if, in its opinion, an instruction given by Controller violates legal provisions (Article 28 (3) sentence 3 GDPR). Processor has the right to suspend the execution of the relevant instruction until it has been confirmed or changed by Controller after verification.

Processor must correct, delete or anonymize or limit the processing of personal data under the contractual relationship if Controller instructs Processor to do so and doing so does not go against the legitimate interests of Processor. If the processor is instructed to delete the data, it is free to anonymise the data. To request automatic anonymization, please contact : datenschutz@raisenow.com.

Processor may only share information about personal data under the contractual relationship with third parties or the data subject after prior instruction or approval by Controller.
Processor hereby agrees that Controller is entitled, generally by appointment, to check compliance with the provisions on data protection and data security as well as the contractual agreements, or to hire a third party to do so, to the appropriate and necessary extent, including but not limited to by obtaining information and access to the stored data and data processing programs as well as through on-site audits and inspections (Art. 28 (3) sentence 2 (h) GDPR).
Processor assures that it will support such checks to the extent necessary.The costs shall be borne by the client.

Processor agrees to maintain confidentiality in the commissioned processing of Controller's personal data. This obligation continues after the end of the Agreement.
Processor guarantees that it will familiarize employees involved in the execution of the work with the data protection rules relevant to their job before commencing the activity and require them to maintain confidentiality during as well as after termination of their employment (Art. 28 (3) sentence 2 (b) and Art. 29 GDPR). Processor will supervise compliance with the data protection regulations within its operation.

The following person is the designated data protection officer for Processor:
Kraska Sebastian
+49 89 189 1736-0
email@iitr.de

Any changes in the identity of the data protection officer are to be communicated to Controller immediately.

6. Notification obligations of Processor in case of processing disruptions and personal data breaches

Processor must inform Controller immediately of any disruptions, violations by Processor or persons employed by Processor of data protection provisions or provisions established in processing requests, and any suspected data breaches or irregularities in the processing of personal data. This applies especially to any reporting or notification obligations of Controller in accordance with Data Protection Acts. Processor agrees to adequately support Controller in performing its duties in accordance with Data Protection Acts. Notifications pursuant to Art. 33 or 34 GDPR on behalf of

Controller may be issued by Processor only after prior instruction in accordance with section 4 of this Agreement.

7. Relationships with subcontractors for core services (Article 28 (3) sentence 2 (d) GDPR)

Processor may engage future subcontractors for processing controller data without separate approval from Controller (Art. 28 (2) sentence 2 GDPR). Processor must ensure that the subcontractor is carefully selected with due regard for the suitability of the technical and organizational measures taken by the subcontractor in accordance with Data Protection Acts.

Currently, the subcontractors listed in Annex 1 are engaged by Processor for the processing of personal data to the extent specified therein.
Controller agrees to the engagement of the subcontractors listed in Annex 1.

Processor must always inform Controller of any intended changes concerning the addition or replacement of subcontractors. Controller will be given the opportunity to object to such changes, provided that the technical and organizational measures agreed to date and promised by Processor cannot be fully guaranteed (Article 28 (2) sentence 2 GDPR). In this case, the intended change is not allowed.

8. Technical and organizational measures according to Art. 32 GDPR (Article 28 (3) sentence 2 (c) GDPR)

A level of security appropriate to the risk for the rights and freedoms of natural persons whose data is subject to processing must be guaranteed. For this purpose, the protection objectives of Art. 32 (1) GDPR, such as the confidentiality, integrity and availability of the systems and services and their resilience in terms of the nature, extent, circumstances and purpose of the processing, must be taken into account in such a way that appropriate technical and organizational remedial measures are taken to permanently reduce the risk. An appropriate and comprehensible methodology that takes into account the likelihood and severity of the risks to the rights and freedoms of the data subjects must be used to assess the risk of the commissioned processing of personal data.

The data protection policy described in Annex 2 details the minimum requirements of the technical and organizational measures appropriate to the identified risk, taking into account the protection objectives based on current technology and with special consideration of the IT systems and processes used by Processor. It also describes the procedure for periodically auditing, measuring and evaluating the effectiveness of the technical and organizational measures to ensure compliance with data protection standards.

9. Obligations of Processor after the end of commissioned processing (Art. 28 (3) sentence 2 (g) GDPR)

After concluding the contractually agreed work, or earlier at request of the Client – at the latest upon termination of the Service Agreement – the Contractor has to hand back to the Client all personal data that came into his possession and is related to the contractual relation or destroy them, upon prior approval, in accordance with data protection principles. A recorded log of the deletion must be presented on request.

Documentation that serves to demonstrate that the processing of data was conducted properly and in accordance with the contract is to be retained by the Contractor in accordance with the respective retention periods beyond the termination of the contract. Alternatively, he may transfer them to the Client at the end of, or on termination of the contract.

10. Miscellaneous

Any special arrangements regarding technical and organizational measures as well as control and audit documentation (including with regard to subcontractors) must be kept on file by both contracting parties for the remainder of their validity and thereafter for three full calendar years. Collateral agreements must generally be set down in writing or a documented electronic format. Should the ownership or the personal data of Controller to be processed by Processor become endangered as a result of third-party measures (such as seizure or attachment), bankruptcy or settlement proceedings or other events, Processor must notify Controller immediately.

Annex 1 – Subcontractors

Currently, the following subcontractor relationships exist in connection with the commissioned processing:

Subcontractors may be eliminated depending on the scope of services.

COMPANY	ADDRESS	SERVICES
Adyen GmbH www.adyen.com	Hackescher Markt 4 Gebäude 44 10178 Berlin Deutschland	Payment Service Provider
Amazon Web Services, Inc. aws.amazon.com/de	Kalanderplatz 1 8045 Zürich, Schweiz eine Zweigniederlassung von AMAZON WEB SERVICES EMEA SARL 38 AVENUE JOHN F. KENNEDY, L-1855 LUXEMBOURG VAT: CHE-430.551.382 MWST	Server / Infrastructure
Datatrans AG www.datatrans.ch	Kreuzbühlstrasse 26 8008 Zürich Schweiz	Payment Service Provider
Stripe Inc. www.stripe.com	185 Berry Street, Suite 550 San Francisco, CA 94107 USA	Payment Service Provider
MNC AG www.mnc.ch	Bahnhofplatz 17 8400 Winterthur Schweiz	Payment Service Provider Text message services
Nine Internet Solutions AG www.nine.ch	Albisriederstrasse 243a 8047 Zürich Schweiz	Server / infrastructure for Peer-to-Peer and Employee Giving
SEPAone www.sepaone.com	Charlottenstrasse 2 10696 Berlin Deutschland	Payment Service Provider

Rackspace International GmbH www.rackspace.com	Pfingstweidstrasse 60 8005 Zürich Schweiz	Server / infrastructure
TWINT AG www.twint.ch	TWINT AGStauffacherstrasse 41CH-8004 Zurich	Payment ServiceProvider
PayPal www.paypal.com	22-24 Boulevard RoyalL-2449 LuxembourgLuxembourg	Payment Service Provider
Elastic elastic.co	Elasticsearch ASPostboks 5391373 Asker, Norway	Server / Infrastructure
Atlassian atlassian.com	Level 6, 341 George Street,Sydney, NSW 2000, Australia	Server / Infrastructure
Wallee en.wallee.com	Neuwiesenstrasse 15CH-8400 Winterthur	Payment ServiceProvider
PostFinance Ltd www.postfinance.ch	PostFinance LtdContact CenterMingerstrasse 203030 Berne	Payment Service Provider / Reconciliation
Ingenico a worldline brand www.ingenico.com	WorldlineRiver Ouest80 Quai Voltaire95870 BezonsFrance	Payment Service Provider
84codes (RabbitMQ) 84codes.com	Hälsingegatan 49113 31 StockholmSweden	Server / Infrastructure
Twilio www.twilio.com	EEA Headquarters25-28 North Wall QuayDublin 1, Irleand	Two Factor Authentication RaiseNow Hub

Annex 2 – Technical and organizational measures/data protection policy

Processor guarantees that it complies with the minimum requirements described below as part of its data protection policy. The policy describes the measures that Processor must take with regard to commissioned processing to ensure the safe the handling of personal data. This data protection policy is based on the Swiss Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR) and other measures that may be requested by the interested parties. Processor is primarily guided by the requirements of Articles 24, 25 and 32 GDPR.

Processor must verify compliance upon request.

1. Confidentiality

1.1 Entry control

The personal data is stored solely on Amazon servers in Frankfurt, on Rackspace servers in London and on nine (nine.ch) servers in Zurich. Amazon and Rackspace are both GDPR-ready and PCI-DSS certified.
https://aws.amazon.com/compliance/pci-dss-level-1-faqs/
https://aws.amazon.com/compliance/gdpr-center/
https://www.rackspace.com/compliance/pci
https://www.rackspace.com/gdpr

1.2 Usage control

A documented, role-based authorization concept must be provided for use of personal data which limits the use so that only authorized individuals can use the personal data necessary for their task (De Minimis Principal). The password rules for access control must also be followed for usage control. Administrative activities must be limited to a small group of administrators. Administrator activities must be monitored and logged to the extent that the effort involved is technically supportable.

1.3 Pseudonymization

Evaluations must be pseudonymized in so far as the connection to the individual is not absolutely necessary for the result.

1.4 Separation control

Measures guaranteeing that data collected for different purposes can be processed separately.
Separation of productive and test system
Data is only collected, stored and processed if it serves the purpose directly.

2. Integrity

2.1 Transfer control

Measures guaranteeing that personal data cannot be read, copied, changed or removed without authorization while being transferred electronically, transported or saved to data media; and that it is possible to verify and establish the bodies to which personal data is to be transmitted using data communication equipment.

The export of personal data is logged

The setting of guidelines for disclosing the data is documented and known to the employees affected

The connection to the database systems is protected

There are rules for data-protection-compliant destruction of data media.

State-of-the-art encryption is used for transfers;

2.2 Input control

Measures ensuring that you can check and determine in retrospect whether personal data was entered into data processing systems, changed or removed, and by whom.

Transparency when data is entered, changed or deleted by individual usernames (logging)

3. Availability and reliability

Measures guaranteeing that personal data is protected against accidental destruction or loss.

A backup concept exists

People responsible and their substitutes are named

Redundant server infrastructure

Procedure for regularly testing, assessing and evaluating (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

Data protection management system implemented;

A security system is in place

Quarterly vulnerability tests and annual check of PCI-DSS SAQ D Level 2

Data-protection-friendly defaults (Art. 25 (2) GDPR)

Anonymization possible at defined intervals

4. Procedures for periodic auditing, measurement and evaluation

A procedure must be implemented for reviewing data protection in the company. It must include the obligation of employees to maintain data secrecy, training and education of employees, and regular auditing of data processing procedures. A complete reporting and management process must be introduced for data breaches and the protection of data subjects' rights. It must also include notification of the Controller.

Annex 3 - Description of transfer and processing

1. Directory of the personal data to be transferred and processed:

- Personal data such as name, address, email, telephone number, date of birth
- Contact preferences, contact details
- Payment-related data such as account number, donation transactions, standing orders and direct debit orders or SEPA mandate, credit card details

2. Purpose of transfer and processing:

The nature and purpose of RaiseNow's processing of personal data arise from the business relationships between customer and contractor.

3. Categories of people affected:

- Supporters (donors, members, sponsors, patrons, mentors, donation collectors)
- Interested parties
- Employees of the client

Data processing contract including Annexures 1 to 3 have been read and understood.

Zürich, 01.04.2023

RaiseNow AG
Jürg Unterweger

RaiseNow AG
Patricia Grossmann