Agreement

Between the responsible person/client:

Example Company, High Street 200, 1234 Example Country

(hereinafter referred to as customer)

And the processor:

rapidmail GmbH, Wentzingerstraße 21, 79106 Freiburg i.Br., Deutschland

(hereinafter referred to as contractor)

the following data processing agreement is made.

Praemble

This agreement is concluded in compliance with the Federal Data Protection Act (BDSG) and the EU General Data Protection Regulation (GDPR) as well as with all other relevant data protection regulations. This agreement is governed by the current laws, as amended from time to time.

This agreement concerns the collection, processing and use of personal data in the sense of the BDSG and GDPR by the contractor on behalf of the client ("order processing"). Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person ("data subject"). The agreement deals with the processing of personal data ("order data").

Against this background, the parties agree as follows:

1. Subject and duration of the contract

(1) Subject

The essential object of the contract is the processing of address data of the client for sending newsletters by e-mail and transactional e-mails. The details of the services result from the General Terms and Conditions of Business (https://www.rapidmail.com/general-terms-and-conditions), which are accepted by the client upon registration. Reference is made here to these services (hereinafter also referred to collectively as the "Service Agreement").

(2) Duration

The term of the present contract shall be governed by the service agreement and the notice periods therein. Any existing contracts for commissioned processing shall be replaced by the conclusion of the present contract.

2. Specification of the content of the order

(1) Nature and purpose of the intended processing of data

The nature and purpose of the processing of personal data by the contractor for the client are specifically described in the service agreement.

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the special requirements of art. 44 et seq. GDPR are met.

(2) Type of data

The object of the processing is personal customer data of the client. The persons affected by the processing of their personal data within the scope of this order are customers, business contacts and interested parties of the client. The types of data processed, as well as the categories of data subjects, are set out in detail in the following section or by selecting the types of data in the digital conclusion of this commissioned processing by the Client.

The subject of the processing of personal data is the following data types/categories (enumeration/description of the data categories)

- ☐ Person master data (contact list of the working group, i.d.R no data subject)
- ☐ Communication data (e.g., telephone, e-mail, social media accounts)
- ☐ Contract master data (contractual relationship, product or contract interest)
- ☐ Content data (e.g. text input, photographs, videos, contents of documents/files),
- ☐ Usage data (e.g. history on our web services, use of certain content, access times),
- ☐ Connection data (e.g. device information, IP addresses, URL referrers), and
- ☐ Location data (e.g. GPS data, IP geolocation, access points)
- ☐ Others

(3) Categories of data subjects

The categories of persons affected by processing include:

- ☐ Employees of the client
- ☐ Customers of the client
- ☐ Suppliers and partners of the client
- ☐ Others

3. Technical-organizational measures

(1) The contractor must document the implementation of the technical and organizational measures set out prior to the award of the contract and prior to processing, in particular with regard to the specific execution of the order, and hand them over to the client for review. If accepted by the client, the documented measures become the basis of the contract. Insofar as the inspection/audit of the client results in a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor has to establish security according to art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with art. 5 para. 1, para. 2 GDPR. Overall, the actions to be taken are data security measures and to ensure a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the costs of implementation and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of art. 32 para. 1 GDPR must be taken into account. [See details in attachment 1].

(3) The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is allowed to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be undershot. Significant changes must be documented.

4. Correction, restriction and deletion of data

(1) The contractor may not correct, delete or restrict the processing of the data processed on behalf of the contract, only on the basis of documented instructions from the client. Insofar as an affected person directly addresses the contractor in this regard, the contractor will immediately forward this request to the client.

(2) Insofar as included in the scope of services, the cancellation concept, the right to be forgotten, rectification, data portability and information according to the client's documented instructions are to be ensured by the contractor directly.

(3) The contractor shall support the customer within the scope of his possibilities in fulfilling the requests obligations set out in Articles 33 to 36 of the GDPR.

(4) The principal alone is responsible for assessing the permissibility of the processing in accordance with Art. 6 Para. 1 GDPR and for safeguarding the rights of the data subjects in accordance with Art. 12 to 22 GDPR. Nevertheless, the contractor is obliged to forward all such inquiries, provided that they are recognizably directed exclusively to the customer, to the customer without delay.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this order, the contractor has statutory obligations according to art. 28 to 33 GDPR; In particular, he ensures compliance with the following requirements:

a) Written appointment of a data protection officer who carries out his activity in accordance with art. 38 and 39 GDPR. As an external data protection officer is:

Mr. Nils Möllers, Keyed GmbH, n.moellers@keyed.de, +49 2505 – 63 97 97

appointed to the contractor. A change of the data protection officer has to be told the client immediately.

b) The preservation of confidentiality under art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. The contractor will use only employees who are committed to confidentiality and who have been previously familiarized with the data protection regulations that are relevant to them. The contractor and any person subordinate to the contractor who has access to personal data may process such data only in accordance with the instructions of the client, including the powers granted in this contract, unless they are required by law to process them.

c) The implementation and compliance with all technical and organizational measures required for this contract in accordance with art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in attachment 1].

d) The client and the contractor cooperate with the supervisory authority on request to fulfill their duties.

e) Immediate information to the client about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies insofar as a competent authority has determined in the context of an administrative or criminal procedure with regard to the processing of personal data in the processing of orders by the contractor.

f) Insofar as the client himself is subject to inspection by the supervisory authority, an administrative offense or criminal proceeding, the liability claim of a data subject or a third party or any other claim in connection with order processing by the contractor, the contractor shall support him to the best of his ability.

g) The contractor shall regularly review the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility complies with the requirements of applicable data protection law and that the protection of the data subject's rights is ensured.

h) Verifiability of the technical and organizational measures taken towards the client within the scope of his control powers according to section 7 of this contract.

i) The Contractor shall take reasonable measures in accordance with the Client's instructions to exclude further unlawful knowledge by third parties and/or to avert further adverse effects on the persons concerned. Pending any instructions from the principal, the contractor shall take all necessary measures to secure data and minimise damage.

j) The Contractor shall support the Customer in complying with its statutory obligations, in particular obligations to ensure the security of personal data, notification obligations in the event of data breaches, information obligations towards affected parties and supervisory authorities, data protection impact assessments and prior consultations. The same shall also apply if the Customer is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or third party or any other claim in connection with the processing of the order. On request, the contractor shall make available to the principal the list of all processing activities to be drawn up by him in accordance with the relevant legal provisions in copied form.

k) The supplier shall inform the contracting authority without delay if he becomes aware of any breaches of the protection of personal data of the contracting authority. The Contractor shall take the necessary measures to secure the data and to mitigate any adverse consequences for the persons concerned and shall consult the Principal without delay.

6. Subcontracting

(1) For the purposes of this regulation, subcontracting means such services which directly relate to the provision of the main service. This does not include ancillary services provided by the contractor, e.g. as a telecommunications services, postal/transport services or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing facilities. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the client's data, even with outsourced ancillary services.

(2) The contractor may only commission subcontractors (other processors) after prior express written consent from the client.

☐ Subcontracting is prohibited.

☒ The client agrees to the assignment of the following subcontractors under the condition of a contractual agreement in accordance with art. 28 para. 2-4 GDPR:

Company subcontractor	**Adress/Country**	**Service**
MEGASPACE Internet Service GmbH	Max-von-Laue-Str. 2b 76829 Landau / Palatinate Germany	The service provided by MEGASPACE is the hosting of the servers at locations within the Federal Republic of Germany.
uvensys GmbH	Robert-Bosch-Straße 4b, 35440 Linden, Hesse, Germany	The service provided by uvensys is the hosting of the servers at locations within the Federal Republic of Germany.

☒ The outsourcing to subcontractors or / the change of the existing subcontractor are permissible insofar as:

- the contractor indicates such outsourcing to subcontractors at least 2 weeks in advance in writing or in text form, and
- the client does not object to the planned outsourcing in writing or in text form until the date of transfer of the data to the contractor and
- a contractual agreement in accordance with art. 28 para. 2-4 GDPR is used.

(3) The transfer of personal data of the client to the subcontractor and its initial action shall only be permitted upon submission of all conditions for subcontracting. Compliance with and implementation of the technical and organisational measures at the subcontractor shall be checked by the contractor in advance of the processing of personal data, taking into account the risk at the subcontractor, and then on a regular basis. The contractor shall make the control results available to the client upon request. The Contractor shall also ensure that the Client can exercise its rights under this Agreement (in particular its control rights) directly against the subcontractors.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that the data protection law is admissible by taking appropriate measures. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Further outsourcing by the subcontractor

☐ is not allowed;

☒ requires the express consent of the main contractor (at least in text form);

The Processor shall ensure that its contractual arrangements with the subcontractor are such that the level of data protection is at least equivalent to the agreement between the Controller and the Processor and that all contractual and legal requirements are complied with; this shall apply in particular also with regard to the use of appropriate technical and organisational measures to ensure an adequate level of security of the processing.

7. Control rights of the client

(1) The client has the right to carry out inspections in consultation with the contractor or to have them carried out by examiners to be named in individual cases. He has the right to satisfy himself of the compliance of this agreement by the contractor in his business through spot checks, which are usually timely to register.

(2) The contractor shall ensure that the client can satisfy himself of the compliance with the obligations of the contractor in accordance with art. 28 GDPR. The contractor undertakes to provide the client with the necessary information to prove the implementation of the technical and organizational measures.

(3) The proof of such measures, which do not concern only the concrete order, can take place for example by

- the certification according to an approved certification procedure according to art. 42 GDPR;
- up-to-date certificates, reports or statements of independent bodies (e.g. auditors, data protection officers, IT security departments, privacy auditors, quality auditors);
- the appropriate certification through IT security or privacy audit (e.g. according to BSI basic protection).

8. Notification in case of violations of the contractor

(1) The contractor supports the client in compliance with art. 32-36 of the GDPR data security obligations, reporting of data breaches, data protection impact assessments and prior consultations. These include

a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights through vulnerabilities, and enable the immediate detection of relevant injury events

b) the obligation to report violations of personal data immediately to the client
c) the obligation to assist the contracting entity in providing information to the person concerned, and to provide him with all relevant information without delay in that connection
d) the support of the client for its data protection impact assessment
e) the assistance of the contracting authority in the context of prior consultations with the supervisory authority

(2) The notification of the responsible person in case of protection violations can be made via the usual (electronic, telephone) communication channels - against the background of the notification obligations, the fastest possible exchange of information is guaranteed.

9. Liability

(1) The Contractor shall be liable to the Client for ensuring that the subcontractor complies with the data protection obligations contractually imposed on it by the Contractor in accordance with this section of the Agreement. The provisions of Art. 82 GDPR shall apply to liability.

(2) The Contractor, its legal representatives or vicarious agents shall not be liable for slight negligence. However, this exclusion of liability in case of slight negligence shall not apply if the breach is of an essential contractual obligation (cardinal obligation). Cardinal obligations or essential contractual obligations are those obligations of the Contractor the fulfilment of which makes the proper performance of this specific Agreement possible in the first place and on the observance of which the Client may regularly rely; i.e. obligations the breach of which would jeopardize the achievement of the purpose of the Agreement.

(3) The parties shall indemnify each other against liability if one party proves that it is not responsible in any respect for the circumstance that caused the damage to a data subject. This shall apply mutatis mutandis in the case of a fine imposed on a party, with the indemnity being to the extent that the other party bears a share of the responsibility for the infringement sanctioned by the fine.

10. Authorization of the client

The Client alone has the authority to make decisions or issue instructions for the commissioned processing. The contractor shall act solely on behalf of and in the interest of the client. The responsibility for compliance with data protection law and the lawfulness of the commissioned processing as well as for safeguarding the rights of the data subjects lies with the Client.

The Contractor shall carry out the commissioned processing exclusively within the scope of the Agreement and in accordance with the Client's written instructions or if there is a legal obligation to process under Union or Member State law to which the processor is subject. The Client shall confirm verbal instructions in text form without delay. The contractor shall not be entitled to make any declarations to the data subjects without the prior consent of the client. In the event of a legal obligation, the Contractor shall inform the Client of this obligation prior to processing.

The contractor may not correct, delete or restrict the processing of the order data on its own authority, but only after receiving written instructions from the client. The Contractor shall immediately inform the Client in writing of all requests and complaints by the data subjects and shall support the Client in safeguarding the rights of the data subjects, such as by notifying them, providing them with information or correcting, blocking and deleting commissioned data.

The parties shall observe the relevant data protection regulations within the scope of the commissioned processing. If the Contractor is of the opinion that an agreement or instruction violates data protection regulations, it shall inform the Client of this in writing without delay. The contractor is entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the client.

11. Deletion and return of personal data

(1) Copies or duplicates of the data are not created without the knowledge of the client. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required for compliance with statutory retention requirements.

(2) After the conclusion of the contractually agreed work or sooner upon request by the client - at the latest upon termination of the service agreement - the contractor shall have all documents, processing results and utilization results (incl. copies) as well as data sets which are related to the contract relationship to hand over client or to destroy it after prior consent in accordance with data protection. The same applies to test and scrap material. The log of the deletion must be submitted on request.

(3) Documentation serving as proof of orderly and proper data processing shall be kept by the contractor according to the respective retention periods beyond the end of the contract. He can hand them over to the client for his discharge at the end of the contract.

(4) The Customer and the Contractor agree on an exclusion of the right of retention under civil law in accordance with § 273 BGB (German Civil Code) to exclude the retention of processed personal data and data carriers in the event of contractual/service disruptions.

12. Secrecy

The contractor will keep the information and documents received in the course of the order processing, in particular the order data, strictly confidential ("business and trade secrets"). The confidentiality obligations shall continue to apply indefinitely even after termination of this agreement.

The duty to maintain secrecy shall not apply or shall cease to exist if the information and documents were already known to the public or the contractor upon conclusion of this agreement or became known to the public after conclusion of this agreement, without the contractor being at fault, or if the contractor is known to a third party, provided the third party does not breach its own confidentiality obligation when handing over the information. The contractor is liable for these facts.

13. Obligation to inform, miscellaneous

(1) Should the Client's data with the Contractor be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client thereof without delay.

The contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the client as the person responsible within the meaning of the General Data Protection Regulation.

(2) Amendments and supplements to this Annex and all its components - including any assurances by the Contractor - require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or supplement to these Terms and Conditions. This also applies to the waiver of this formal requirement.

(3) In the event of any contradictions, the provisions of this Annex on data protection shall take precedence over the provisions of the contract. Should individual parts of this Annex be invalid, this shall not affect the validity of the rest of the Annex.

(4) German law shall apply. The place of jurisdiction is Freiburg i.Br. (79106).

This document is to inform you about the measures taken in connection with personal data processing operations.

“Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk” (Art. 32 (1) GDPR).

Controller:	rapidmail GmbH
Address:	Wentzingerstrasse 21, 79106 Freiburg im Breisgau, Germany
Data protection officer:	Nils Möllers
IT Officer:	Mr. Sven Kummer
Date:	5/23/2022

Basic information

☒ A data protection officer has been duly appointed.

☒ Employees are bound to confidentiality (Art. 32 (1) (b) GDPR).

☒ Employees are regularly instructed on the protection of personal data.

☒ There is an up-to-date record of processing activities (Art. 30 GDPR).

---

1. Measures to ensure confidentiality

1.1 Physical access (Access to premises must be protected)

☒ Use of authorization passes.

☒ Use of electronic access code cards/access transponders.

☒ Existence of an access authorization concept.

☒ Use of video surveillance to control physical access.

☒ Use of an alarm system.

☒ Fence around the data center.

☒ Any access to the data center is time-logged and evaluated.

☒ There is a rule/concept about keys.

☒ Use of visitor ID cards.

☒ Visitors escorted by company employees or security personnel.

☒ Security also outside working hours by (24/7) plant security.

☒ Special glass for sensitive areas or to shield against third-party inspection.

☒ Separately protected physical access to server environments and the data center.

1.2 System access (Unauthorized access to and use of IT systems must be prevented)

☒ Use of suitable network encryption.

☒ Password protection for computer workstations.

☒ Use of individual passwords and prevention of group passwords.

☒ Automatic password-secured screen locking after inactivity (screen saver).

☒ Automatic locking of user accounts after multiple incorrect password entries.

☒ Use of a password policy that requires secure password complexity.

☒ Process for assigning rights when new employees join the company.

☒ Process for revoking rights when employees change departments.

☒ Process for revoking rights when employees leave the company.

1.3 Data access (Unauthorized activities in IT systems outside of granted authorizations must be prevented)

☒ Use of an authorization concept that transparently controls access for all employees and service providers.

☒ Definition of power to enter, change, and/or erase data in accordance with the roles & authorizations concept.

☒ Regular review of authorizations.

☒ Logging of accesses to customer systems.

☒ Logging of erasures on the instructions of the controller (Client).

☒ Use of an anti-virus protection solution on each end device.

☒ Use of a firewall including spam protection.

☒ SSL encryption for importing/exporting data from rapidmail.

1.4 Compliance with instructions (Steps must be taken to ensure that service providers who process data on behalf of the Client only process data in accordance with the Client's instructions)

☒ Drafting of contracts for contract processing in accordance with legal requirements (Art. 28 GDPR).

☒ Central recording of existing service providers and contract processors.

☒ Controls of the technical and organizational measures are carried out before the start of processing.

1.5 Separation (Steps must be taken to ensure that data collected for different purposes, persons, and companies can be processed separately from each other)

☒ Separation of customers (multi-tenancy capability of the systems used).

☒ Logical data separation (e.g., based on customer or tenant numbers) in databases.

☒ Authorization concept that takes into account the separate processing of Client data from data of other customers.

☒ Separation of development, test, and production systems.

2. Measures to ensure integrity

2.1. Disclosure/transmission (Aspects of the disclosure (transmission) of personal data must be regulated: electronic transmission, data transport, and their control)

☒ There is a secure method of sending data between the Client, Contractor and third parties.

☒ Encrypted ZIP files are possible for email transmission.

☒ Use of VPN connections.

☒ Data exchange takes place via SSL (https) encryption.

☒ Documented management of mobile end devices and data storage media.

☒ Safe disposal/secure erasure of data storage media has been ensured.

☒ Use of document shredders (in accordance with DIN 66399).

2.2 Entry (Steps must be taken to ensure that data management and maintenance are traceable and documented)

☒ Identification of recorded data.

☒ Logging of entries/erasures.

☒ Use of a log evaluation system.

☒ Regulations on retention periods for auditing/evidence purposes (4 weeks).

3. Measures to ensure availability

3.1 Availability (Data must be protected against accidental destruction or loss)

☒ Data protection and backup concepts are in place. Data protection is checked in regular test routines, thereby ensuring that various backup versions can be restored.

☒ Daily execution of data protection and backup concepts for data and systems (bare metal restore).

☒ Access to server premises limited to necessary personnel.

☒ Fire alarm systems in server premises or in the data center.

☒ Smoke detectors in server premises or in the data center.

☒ Waterless firefighting systems in server premises or in the data center.

☒ Air-conditioned server premises.

☒ Lightning/surge protection.

☒ Server premises in separate fire compartment.

☒ Accommodation of encrypted backup systems (rijndael-256/AES) in separate premises and fire compartment.

☒ Disaster or emergency plan (e.g., water, fire, explosion, threat of attack, crash, earthquake).

☒ UPS (uninterruptible power supply) system.

☒ Use of a power generator during power outages.

4. Measures to ensure resilience

4.1. Resilience and fail-safe operation

☒ Backup data centers/servers are available.

☒ Redundant data connection.

☒ Data storage on RAID systems (RAID 1 and higher).

☒ Performance of penetration tests by independent entity (OPTIMA Business Information Technology GmbH).

☒ Communication channel with manufacturers to find out about new updates and patches that have been released for the devices in possession.

☒ Definition of periods during which the updates are to be implemented (periods of reduced operations, maintenance periods, etc.).

☒ Definition of a test period to verify the correct implementation of the update and to ensure that operations continue to run smoothly with the new updates.

☒ Limitation of authorizations based on need.

☒ Performance of a risk analysis, taking into account all these systems, devices, and assets that have been identified to determine the threats, including their likelihood and impact.

☒ Use of cyber insurance to cover risks that do not have technical security measures in place, specifying scope, indemnities, and coverage exceptions.

5. Measures for regular monitoring, assessment and evaluation

5.1 Control procedures

☒ Notification of new/modified data processing procedures to the data protection officer.

☒ Processes for reporting new/modified procedures are documented.

☒ Security measures taken are subject to regular internal control.

☒ A process is in place to prepare for security breaches (attacks) and system malfunctions and to identify, contain, eliminate, and recover from them (incident response process).

☒ A data protection management system is in place.

These technical and organizational measures are continuously audited at regular intervals by **Keyed GmbH**. As a result, rapidmail guarantees a very high level of protection for the systems that form part of processing operations.