Agreement regarding the processing of personal data (according to the GDPR) between

CleverReach GmbH & Co. KG
Schafjückenweg 2
26180 Rastede

- hereinafter referred to as Processor -

and

- hereinafter referred to as Controller -

1 Subject and duration of the contract

(1) The Processor shall perform the services described in Annex 1 for the Controller bound by contract. The subject matter, purpose and way of data processing, as well as the specifications of the processed data are described therein.

(2) As long as nothing else is agreed on, this Agreement shall become effective after it has been signed by both parties. It shall remain effective for as long as the Processor processes personal data for the Controller. This Agreement supersedes any previous agreements for data processing on behalf between the Parties, if any.

2 Instructions by the Controller

(1) The Controller is responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of the processing and for the protection of the data subject rights. Statutory or contractual liability regulations shall remain unaffected.

(2) The Processor shall process the personal data made available exclusively in accordance with the instructions of the Controller and within the scope of the contractual Agreement. Commissioned processing of data includes correction, deletion and blocking only if instructed to do so by the Controller. In exceptional cases, the Processor as a sender may deviate from this agreement by correcting, deleting or blocking data that it processes on behalf of the client if for legal reasons it is obliged to remove e-mail addresses from the database and to place them on a blacklist, if an email to a specific and identical email address returns three times consecutively as undeliverable (so-called hard bounces) or if there are complaints from email recipients.

(3) Processing shall only be carried out when this is requested by the Controller, unless the Processor is obliged to process such data by the law of the European Union or of the Member States to which the Processor is subject. If this is the case, the Processor shall inform the Controller of such legal requirements prior to processing, unless the relevant law prohibits such communication because of an important public interest.

(4) Instructions can generally be given orally. Oral instructions must then be documented by the Controller. Instructions must be given in writing or in text form if requested by the Processor.

(5) If the Processor is of the opinion that a directive by the Controller violates data protection regulations, it must inform the Controller without delay.

3 Technical and organizational measures

(1) The Processor undertakes to implement appropriate technical and organizational security measures for the data to be processed and to document them in Annex 3 to this Agreement. The security measures shall at all times ensure a level of protection appropriate to the risk. When assessing the appropriate level of protection, the parties shall take into account the state of the art, the cost of implementation, the nature, scope, circumstances, purposes of the processing and the categories of data (in particular pursuant to Article 9 (1) or Article 10 of the GDPR) as well as the different probabilities of occurrence and the severity of the risk for the data subjects.

(2) Over time, the measures taken must be adapted to technical and organizational developments. Their effectiveness shall be regularly reviewed, assessed and evaluated. The Processor may only make adjustments if they at least reach the same level of security as the previous measures. Unless specified differently, the Processor must only notify the Controller of significant adjustments.

(3) The Processor shall support the Controller in complying with all legal obligations regarding technical and organizational measures. Upon request, the Processor shall assist in the preparation and updating of the list of processing activities of the Controller. The Processor will assist in the preparation of a privacy impact assessment and, if appropriate, in the prior consultation of the supervisory authorities. The Processor shall disclose all necessary information and documents to the Controller on request.

4 Obligations of the Processor

(1) The Processor confirms that it is aware of the prevailing data protection regulations and that it implements them. It shall organize the internal organization within its area of responsibility in a way that meets the special requirements of data protection.

(2) The Processor provides adequate guarantees that appropriate technical and organizational measures are in place to ensure that the processing complies with the data protection rules and the rights of the data subject.

(3) The Processor warrants that it will familiarize the personnel involved in the performance of the work with the applicable data protection provisions and that persons authorized to process the personal data are bound by confidentiality or are subject to an appropriate statutory confidentiality obligation. It monitors compliance with data protection regulations.

(4) The Processor may access personal data of the Controller for purposes of data processing on behalf only if this is indispensable for processing the data.

(5) If required by law, the Processor will appoint a data protection officer. The contact details of the data protection officer will be communicated to the Controller to enable direct contact.

(6) The Processor may process the personal data provided to it exclusively in the territory of the Federal Republic of Germany or in a member state of the European Union. Processing personal data in a third country requires the Controller's prior documented approval and may only be done when the special legal requirements of the GDPR are complied with.

(7) In the event of subcontracting involving a transfer of personal data within the meaning of Chapter V of the GDPR, the Processor shall ensure compliance with the provisions of Articles 44 et seq. of the GDPR by providing appropriate safeguards, if necessary, that are in accordance with Article 46 of the GDPR. If the Processor uses a sub-processor where the processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the Processor undertakes to conclude standard contractual clauses with said sub-processor in accordance with Article 46 of the GDPR, if the conditions for the application of these standard contractual clauses are met.

(8) The Processor shall support the Controller, inter alia with appropriate technical and organizational measures, so that they can fulfill their existing obligations under data protection law towards the data subject, e.g. the information and disclosure to the data subject, the correction or deletion of data, the restriction of processing or the right to data transfer and objection. In consideration of the nature of processing and the information available, the Processor shall assist in carrying out a data protection impact assessment and in any necessary consultation with supervisory authorities and in fulfilling its obligation to respond to requests from Data Subjects to exercise their rights. The Processor shall inform the Controller without undue delay of any assertion of rights by Data Subjects affected by the Data Processing Activities. The Processor shall designate a contact person to assist the Controller in fulfilling statutory duties to provide information and disclosure that arise in connection with the commissioned processing and shall notify the Controller of the contact person's contact details without undue delay. If the Controller is subject to special statutory duties to provide information in the event of unlawful acquisition of data, the Processor shall support the Controller in this regard. The Processor may only provide information to the Data Subject or third parties after prior instruction by the Controller. If a Data Subject asserts its rights under data protection law directly against the Processor, the Processor shall immediately forward this request to the Controller so that they can review these rights and implement them accordingly.

5 Authorization for subcontracting

(1) The Processor may only commission subcontractors if it informs the Controller in advance of any intended change with regard to the involvement or replacement of other data processors, which gives the Controller the opportunity to object to such changes within 30 days. The objection must be made in written form and may only be made for good reasons, for example when provisions of the data protection law are violated.

(2) Subcontracting relationships include, but are not limited to, relationships where the Processor asks other processors to perform the services to which this Agreement refers, whether in part or as a whole. Ancillary services for which the Processor uses third parties to support the execution of the order are not considered as subcontracting relationships within the meaning of this provision. These include e.g. telecommunications services, services for IT security, or cleaning staff. However, the Processor shall be obliged to enter into appropriate and legally compliant contractual agreements and to take control measures in order to ensure the protection and security of the Controller's data also for outsourced ancillary services.

(3) The subcontractor may only access the data if the Processor ensures, by means of a written contract, that the regulations agreed in this Agreement also apply to the subcontractors. In particular, sufficient guarantees must be offered that the appropriate technical and organisational measures are carried out in such a way that the processing takes place in accordance with the data protection regulations.

(4) The use of the subcontractors listed in Annex 2 at the time of signing the Agreement shall be deemed to have been approved provided that the conditions specified in Section 5 (3) of this Agreement are met.

6 Monitoring rights of the Controller

The Processor agrees that the Controller or a person commissioned by the Controller shall be entitled to monitor compliance with the provisions on data protection and the contractual agreements to the necessary extent, in particular by obtaining information and requesting relevant documents or access to the Processor's offices during the designated business hours after prior notification. Suitable and valid certificates for IT security (e.g. IT Baseline Protection, ISO 27001) or for data protection (e.g. Art. 42 of the GDPR) can also provide evidence of proper processing, provided that the respective subject of the certification also applies to the commissioned processing in the specific case. However, the presentation of a relevant certificate does not substitute the obligation of the Processor to document the security measures within the meaning of Section 3 of this Agreement.

7 Processor's violations

The Processor shall immediately inform the Controller of any disruptions in the course of operations which entail risks for the Controller's data. The same applies in the event of suspected breaches of data protection in connection with the Controller's data. This also applies if the Processor becomes aware that its security measures do not meet the statutory requirements. The Processor understands that it is obligated to document all violations of the protection of personal data and report them to the supervisory authorities or the data subject. In case such violations have occurred, the Processor shall support the Controller in complying with their reporting and notification obligations in an appropriate manner. The Processor shall report the violations of the Controller without delay and provide at least the following information:

a) a description of the nature of the injury, the categories and the approximate number of persons and records affected,

b) name and contact details of a contact person for further information,

c) a description of the likely consequences of the injury, and

d) a description of the measures taken to remedy or mitigate the violation.

8 Termination

(1) After completion of the commissioned processing, the Processor shall either delete or return all personal data at the discretion of the Controller, unless there is a legal obligation to store the personal data. This also applies to any backup copies in accordance with the technical and organizational measures taken.

(2) The Controller may terminate this Agreement without notice if the Processor seriously violates the provisions of this agreement or the data protection regulations and the Controller cannot be reasonably expected to continue the cooperation with the Processor until the end of the notice period or until the agreed end of the work.

(3) The Processor may terminate the contractual relationship without notice if the Controller insists on the fulfillment of its instructions, even though these instructions violate applicable legal requirements or this contract and the Processor has informed the Controller thereof.

9 Final provisions

(1) If the Controller's property is endangered by third-party measures (such as seizure or confiscation), insolvency proceedings or other events, the Processor must inform the Controller immediately. Any right of retention is excluded with respect to the disks and data of the Controller.

(2) The establishment of the Agreement, amendments to the Agreement and any ancillary agreements must be drawn up in writing. From 25 May 2018, this can also be done electronically.

(3) If any part of this Agreement should prove legally ineffective, this shall not affect the effectiveness of the Agreement.

(4) If legally permissible, the parties agree that the place of jurisdiction shall be the registered office of the Processor.

Place, Date	Place, Date
____________________________	Rastede, ______________
Signature of Controller	Signature of Processor
____________________________	______________________
	Management

Annex 1: List of commissioned services and contact details of the data protection officer

Object of the processing	Provision of the CleverReach software for email dispatch/evaluation and management by the Controller. In addition, at the request of the Controller for remote maintenance, access to productive systems of the Controller and execution of support work within these systems by the Processor (associated with this: possible access to personal data for the Processor).

Nature and purpose of processing	Collection, storage, use, processing and transmission of the Controller's account data and user management data. Storage, processing, and transmission of recipient data for the purpose of sending/evaluating emails. Upon request of the Controller for remote maintenance, the Controller shall also provide the Processor with FTP access data to their productive systems. In accordance with this Agreement, the Processor shall access the systems using the provided access data and shall perform support work in order to determine an error that has occurred in connection with the use of the CleverReach Software by the Controller and to be able to remedy it quickly and effectively.

Type of personal data	Account data of the Controller - Form of address - Name and surname - E-addresses of the users in the account - Company, invoice address Recipient details (email address, first name and surname) - E-mail address - Name and surname - Street address - IP addresses of the recipients when tracking is enabled Data in the productive systems (on request for remote maintenance) Contract
Categories of data subjects	- Contact persons/acting persons on the side of the Controller - Newsletter recipients who may be buyers, customers, prospects, or members, depending on the Controller's offerings and services

Name and contact details of the data protection officer of the Controller (if existing)	
Name and contact details of the data protection officer of the Processor	Dr. Uwe Schläger, datenschutz nord GmbH datenschutz nord GmbH Konsul-Smidt-Str. 88 28217 Bremen Germany Contact: Conrad S. Conrad, Legal advisor E-mail: cconrad@datenschutz-nord.de

Annex 2: List of subcontractors including processing sites

Subcontractor (name, legal form, registered office of the company)	**Processing site**	**Type of service**
PlusServer GmbH	Germany	E-mail dispatch
Amazon Web Services, Inc.	Ireland Germany	Data storage and processing, E-mail dispatch
Hetzner Online GmbH	Germany	E-mail dispatch

Annex 3: Technical and organizational measures at CleverReach GmbH & Co. KG

A Measures to ensure confidentiality and integrity (1.1 Site 1)

1.	**Access control measures to server rooms**
1.1	Is personal data stored on servers operated by you? ☒ Yes ☐ No
1.2	Please specify the site of the server room/data center (DC). **Site 1**: Germany - **no data is stored here** **Site 2**: Amazon Web Services, Inc., Ireland **Site 3**: PlusServer GmbH, Germany **Site 4**: Amazon Web Services, Inc., Germany **Site 5**: Hetzner Online GmbH, Germany Relevant data protection contracts have been concluded with all external service providers in accordance with Art. 28 of the GDPR, or recognized safeguards have been implemented in accordance with Art. 46 of the GDPR (i.a. through the conclusion of standard contractual clauses ((EU) 2021/914 of 06/04/2021)). In the case of transfers to the USA, an adequate level of data protection is ensured by the certification of the provider Amazon Web Services, Inc. in accordance with the adequacy decision (EU-U.S. data protection framework). For specific data processing by external service providers, their respective self-implemented technical-organizational measures apply, to which we refer. The data protection agreements with the external service providers are regularly reviewed and adapted to the legal situation.
1.3	Is the personal data distributed to more than one server site/data center (e.g. backup server/use of cloud services)? ☒ Yes ☐ No
1.4	**If 1.3 yes: Please also provide the corresponding site information for other servers.** Other sites: Amazon Web Services, Inc., Ireland
1.5	Are the following information on access control measures valid for **all** server/data center sites in use? ☐ Yes ☒ No, only for site 1
1.6	Is the server room windowless? ☒ Yes ☐ No
1.7	Is the server room alarmed by means of a burglar alarm system (EMA)? ☒ Yes ☐ No
1.8	If 1.7 yes: Who is informed when the EMA is triggered? ☒ Assigned security ☐ Administrator ☒ Management board ☒ Miscellaneous: Police
1.9	Is the server room video monitored? ☐ Yes, without image ☐ Yes, with image ☒ No
1.10	How many people have access to the server room and what are their functions? Number of persons: 8 Role in the organization: Administrators, Head of IT, Management board

1.11	Is the server room equipped with an electronic locking system? ☒ Yes ☐ No, with mechanical lock
1.12	How many keys to the server room exist, who issues the keys? Number of keys: 8 Issuer: Administrator
1.13	What material is the access door to the server room made of? ☒ Steel/Metal/ Fire door wood T-30 ☐ Other material
1.14	Is the server room used for purposes other than its actual function? ☐ Yes ☒ No
2.	**Measures for controlling access to offices**
2.1	Location of the client workstations from which personal data is accessed: Workplaces of the employees
2.2	Is there a porter service/permanently staffed reception area to the building or your offices? ☒ Yes ☐ No
2.3	Is a visitor's book kept? ☒ Yes ☐ No
2.4	Is the building or are the offices protected by a burglar alarm system (EMA)? ☒ Yes ☐ No
2.5	Who is informed when the EMA is triggered? ☒ Assigned security ☐ Administrator ☒ Management board ☒ Miscellaneous: Police
2.6	Are the office building or its entrances monitored by video? ☐ Yes, without image recording ☐ Yes, with image recording ☒ No
2.7	Are the building/offices equipped with an electronic locking system? ☒ Yes, buildings and offices are electronically locked ☐ Yes, but only the building, not the entrance to the offices or to the office floor. ☐ Yes, but only the entrance to the offices/to the office floor, not the building as a whole. ☐ No
2.8	**If 2.7 yes**: Which access technology is used? ☒ RFID ☒ PIN ☐ Biometry ☐ Other:
2.9	**If 2.7 yes**: Are access rights personalized? ☒ Yes ☐ No
2.10	**If 2.7 yes**: Are access attempts logged by the access system? ☒ Yes, both successful and unsuccessful access attempts ☐ Yes, but only successful positive accesses ☐ Yes, but only unsuccessful access attempts ☐ No, the lock will only be released or not
2.11	**If 2.10 yes**: How long is this log data kept? 6 months

2.12	**If 2.10 yes**: Are the logs evaluated regularly? ☐ Yes ☒ No, but evaluation is possible if necessary
2.13	Is there a mechanical lock for the buildings? ☒ Yes ☐ No
2.14	**If 2.13 yes**: Is key issuing logged, who hands out the keys? ☒ Yes ☐ No issuing office: Management board
2.15	Are there official access regulations for external individuals (e.g. visitors) to the offices? ☐ No ☒ Yes, external individuals will be picked up at the entrance or reception by the contact person and may only move around the building if accompanied.
3	**Access control measures**
3.1	Is there a process for assigning user IDs and access authorizations when hiring new employees, when employees leave or when making organizational changes? ☒ Defined release process ☐ No defined release process, on demand ☐ Other assignment procedure:
3.2	Is the assignment of, or change to, access authorizations logged? ☒ Yes ☐ No
3.3	Do employees authenticate themselves to the central directory service using a unique ID? ☒ Yes ☐ No
3.4	Does the organization have binding password parameters? ☒ Yes ☐ No
3.5	What are the password requirements for access to the processed data? **PW length:** ☒ 10 characters or more ☐ Less than 8 characters ☐ Less than 6 characters **Which character types must be present?** ☐ Special characters ☒ Digits ☒ Upper/lower case **Period of validity of the PW:** ☐ 90 days or less ☐ 180 days or less ☒ More than 180 days
3.6	Does the IT system force the user to comply with the above PW specifications? ☒ Yes ☐ No
3.7	Is the screen locked when the user is inactive? ☒ Yes ☐ No If yes, after how many minutes? After 10 minutes
3.8	What actions do you take if a password is lost, forgotten or exposed? ☒ Admin assigns new initial password ☐ None
3.9	Is there a limit to the number of unsuccessful login attempts? ☒ Yes, after 3 tries ☐ No

3.10	**If 3.9 yes**, how long does access remain blocked if the maximum number of unsuccessful login attempts is reached? ☐ Access remains blocked until the block is manually released ☒ Access remains blocked for 10 minutes.
3.11	How is authentication performed for remote access: Authentication with ☐ Token ☒ VPN Certificate ☐ Password
3.12	Is there a limit to unsuccessful login attempts for remote access? ☐ Yes ☒ No, a login attempt is not possible without a certificate
3.13	Is remote access automatically disconnected after a certain period of inactivity? ☒ Yes, after 30 minutes ☐ No
3.14	Are the systems protected by a firewall? ☒ Yes ☐ No
3.15	**If 3.14 yes:** Is the firewall updated regularly? ☒ Yes ☐ No
3.16	If 3.14 yes: Who administers your firewall? ☒ Own IT ☐ External service provider
4	**Measures to secure paper documents, mobile media and mobile terminals**
4.1	How are paper documents containing personal data that are no longer required disposed of (e.g. printouts/files/correspondence)? ☐ Waste paper/residual waste ☒ Shredders are available for this purpose and their use is mandatory. ☒ The Controller's order data is not available in paper form.
4.2	How are media containing personal data (USB sticks, hard disks) disposed of which are no longer required? ☒ Physical destruction by own IT. ☐ Physical destruction by external service provider. ☐ Deleting the data
4.3	Does the organization allow the use of mobile media (e.g. USB sticks)? ☒ Yes, but only media provided by the Processor ☐ No
4.4	Are employees allowed to use private media (e.g. USB sticks)? ☐ Generally yes ☐ Yes, but only after approval and verification of the storage medium by IT. ☒ No, all required storage media are provided by the Processor.
4.5	Is the Controller's data also processed on mobile devices by employees? ☒ Yes, but only on instruction of the Controller and on devices of the Processor ☐ No
4.6	Do employees also process personal data on their own private devices (BYOD)? ☐ Yes ☒ No

5	**Measures for secure data transmission**
5.1	Is the transfer of personal data encrypted end to end? ☐ Not at all ☐ No, data transfer via MPLS ☐ Encrypted file is sent as an e-mail attachment ☐ PGP/SMime ☐ Encrypted media ☐ VPN ☒ SSL/TLS ☒ SFTP ☐ Other:
5.2	Who manages the keys and certificates? ☐ User ☒ Own IT ☐ External service provider
5.2	Are transmission processes logged? ☒ Yes ☐ No
5.3	**If 5.2 yes**: How long is this log data kept? Permanently
5.4	**If 5.2 yes**: Are the logs evaluated regularly? ☐ Yes ☒ No, but evaluation is possible if necessary

B. Measures to ensure availability (A 1.1 Site 1)

1.	Server room
1.1	Does the server room have a fire-resistant or fire-retardant access door? ☒ Yes ☐ No
1.2	Is the server room equipped with smoke detectors? ☒ Yes ☐ No
1.3	Is the server room connected to a fire alarm center? ☒ Yes ☐ No
1.4	Is the server room equipped with fire extinguishing systems? ☒ Yes, CO2 fire extinguisher ☐ Yes, Halon/Argon extinguisher ☐ No
1.5	What are the outer walls of the server room made of? ☐ Solid wall (e.g. concrete, brick wall) ☐ Lightweight construction ☒ Fire protection wall (e.g. F90)
1.6	Is the server room air-conditioned? ☒ Yes ☐ No
1.7	Does the server room have an uninterruptible power supply (UPS)? ☒ Yes ☐ No
1.8	Is the power supply of the server room additionally secured by a diesel generator? ☐ Yes ☒ No
1.9	Are functionalities 1.2, 1.3, 1.4, 1.7 and 1.8 tested regularly? ☒ Yes ☐ No
2	**Backup and emergency concept, virus protection**
2.1	Is there a backup concept? ☒ Yes ☐ No
2.2	Is the backup recovery functionality tested regularly? ☒ Yes ☐ No

2.3	How often are backups made of the system on which personal data is stored? ☒ Real-time mirroring ☒ Daily ☐ One to three times a week
2.4	What backup media are backups stored on? ☒ Second redundant server ☐ Backup tapes ☐ Hard disks
2.5	Where are the backups stored? ☒ Second redundant server at a different location ☐ Safe (fireproof, safe for media and documents) ☐ Locked filing cabinet/desk ☐ In the server room
2.6	Are the backups encrypted? ☒ Yes ☐ No
2.7	Is the location of the backups in a fire compartment or building section separate from the primary server? ☒ Yes ☐ No
2.8	Is a documented process for software or patch management in place? ☒ Yes ☐ No ☐ Process exists, but is not documented
2.9	**If 2.8 yes**, who is responsible for software and patch management? ☐ User ☒ Own IT ☐ External service provider
2.10	Is there an emergency concept (e.g. emergency measures in case of hardware defects/fire/total loss etc.)? ☒ Yes ☐ No
2.11	Are the IT systems technically protected against data loss/unauthorized data access? Yes, by means of always updated ☒ Virus protection ☒ Anti-Spyware ☒ Spam filter ☒ Firewall ☒ Backup
2.12	**If 2.11 yes**, who is responsible for the current virus protection, anti-spyware and spam filters? ☐ User ☒ Own IT ☐ External service provider
3	**Internet connection**
3.1	Does the organization have a redundant Internet connection? ☐ Yes ☒ No
3.2	Are the individual sites of the company redundantly connected to each other? ☒ Yes ☐ No
3.3	Who is responsible for the company's network connection? ☒ Own IT ☐ External service provider

C. Other measures according to Art. 32 (1) (b, c, d) GDPR

1.	**Resilience**
	Are there measures in place to ensure the ability to sustain the resilience of the systems and services associated with the processing? ☒ yes ☐ no The Processor's IT administration shall carry out regular stress and performance tests in order to maintain order processing and the Processor's state-of-the-art systems.
2	**Recoverability**
	Are there emergency or recovery policies and measures in place to ensure the ability to rapidly restore the availability of and access to personal data in the event of a physical or technical incident? ☒ yes ☐ no
3	**Procedures for reviewing and evaluating the measures taken**
3.1	Is there a procedure for regularly reviewing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing? ☒ yes ☐ no In collaboration with the data protection officer of the Processor, the technical and organizational measures are documented continuously, checked and evaluated annually and, if necessary, are adjusted according to the current state of technology.
3.2	Is a data protection management tool used? ☒ yes ☐ no The data protection management tool is used to document all procedures and processes (e.g. list of processing activities, data breakdown reports and enquiries from data subjects) as well as their evaluation.
3.3	Is there a documented policy for dealing with data breaches? ☒ yes ☐ no
3.4	Is there a list of processing activities? ☒ yes ☐ no