**Annex to the Customer Agreement on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR).**

concluded by and between

**[COMPANY/ORGANIZATION NAME]**

**[COMPANY /ORGANIZATION ADDRESS]**

(hereinafter referred to as the “Customer”)

and

digital publishing AG / Speexx

Tumblingerstraße 32

80337 München

(hereinafter referred to as “Speexx”).

This annex details the parties’ obligations on the protection of personal data, associated with the processing of personal data on behalf of the Customer as a data controller, and described in detail in the Customer Agreement dated xxx (hereinafter, the “Customer Agreement”). Its regulations shall apply to any and all activities associated with the Customer Agreement, in whose scope Speexx’s employees process the Customer’s data (hereinafter, “Data”) on behalf of the Customer as a controller (hereinafter, “Contract Processing”).

**§ 1 Scope, duration and specification of Contract Processing of Data**

1. The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Customer Agreement. Specifically, Contract Processing shall include, but not be limited to, the following Data:

|  |  |  |
| --- | --- | --- |
| **Type of data** | **Type and purpose of Contract Processing** | **Categories of data subjects affected** |
| Private/business contact details or identification details provided by the Customer or the data subject: first name, last name, gender, email address, telephone number, nick name, time zone, content and learning preferences | Speexx operates a cloud-based online platform for language learning solutions, including assessment, self-learning and productivity tools, as well as synchronous and asynchronous training services with a trainer via integrated communication channels (chat, virtual classroom) or phone and email. To provide access to the platform and the services, The Customer or the data subject provides Speexx data subject contact details to give access to the Speexx platform and related training services. | Customer’s employees  Customer’s applicants |

**§ 2 Scope of application and responsibilities**

Speexx shall process Data on behalf of the Customer. Such Contract Processing shall include all activities related to the Service detailed in the Customer Agreement. Within the scope of this annex, Customer shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Speexx and the lawfulness of having Data processed on behalf of the Customer. Customer shall be the “controller” in accordance with Article 4 no. 7 of the GDPR.

**§ 3 Speexx’s obligations**

1. Except where expressly permitted by Article 28 (3)(a) of the GDPR, Speexx shall process data subjects’ Data only within the scope of the Customer Agreement. Where Speexx believes that an instruction would be in breach of applicable law, Speexx shall notify the Customer of such belief without undue delay. Speexx shall be entitled to suspending performance on such instruction until the Customer confirms or modifies such instruction.
2. Speexx shall, within Speexx’s scope of responsibility, organise Speexx’s internal organisation so it satisfies the specific requirements of data protection. Speexx shall implement technical and organisational measures to ensure the adequate protection of the Customer’s Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Speexx shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. The Customer is familiar with these technical and organisational measures, and it shall be the Customer’s responsibility that such measures ensure a level of security appropriate to the risk.

Speexx reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

The Speexx technical and organizational measures are listed under “Technical and Organisational Measures” of this annex.

1. Speexx shall support the Customer, insofar as is agreed upon by the parties, and where possible for Speexx, in fulfilling data subjects’ requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR.
2. Speexx warrants that all employees involved in Contract Processing of the Customer’s Data and other such persons as may be involved in Contract Processing within Speexx’s scope of responsibility shall be prohibited from processing Data outside the scope of the Customer Agreement. Furthermore, Speexx warrants that any person entitled to process Data on behalf of Customer has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
3. Speexx shall notify the Customer, without undue delay, if Speexx becomes aware of breaches of the protection of personal data within Speexx’s scope of responsibility. Speexx shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; Speexx shall coordinate such efforts with the Customer without undue delay.
4. Speexx shall appoint a data protection officer for any issues related to data protection arising out of or in connection with the Customer Agreement. The appointed data protection officer is:

Felix Frankenberger, Data Protection Officer, +498974748248, f.frankenberger@speexx.com

1. Speexx warrants that Speexx fulfils its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. Speexx shall correct or erase Data if so instructed by the Customer and where covered by the scope of the Customer Agreement. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Speexx shall, based on Customer’s instructions, and unless agreed upon differently in the Customer Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Customer.
3. Speexx shall, upon termination of Contract Processing and upon Customer’s instruction, return all Data, carrier media and other materials to Customer or delete the same.
4. Where a data subject asserts any claims against the Customer in accordance with Article 82 of the GDPR, Speexx shall support the Customer in defending against such claims, where possible.

**§ 4 Customer’s obligations**

1. The Customer shall notify Speexx, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by the Customer in the results of Speexx’s work.
2. Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Speexx in accordance with Article 82 of the GDPR.
3. The Customer shall notify to Speexx the point of contact for any issues related to data protection arising out of or in connection with the Customer Agreement.

**§ 5 Enquiries by data subjects**

1. Where a data subject asserts claims for rectification, erasure or access against Speexx, and where Speexx is able to correlate the data subject to the Customer, based on the information provided by the data subject, Speexx shall refer such data subject to the Customer. Speexx shall forward the data subject’s claim to the Customer without undue delay. Speexx shall support the Customer, where possible, and based upon the Customer’s instruction insofar as agreed upon. Speexx shall not be liable in cases where the Customer fails to respond to the data subject’s request in total, correctly, or in a timely manner.

**§ 6 Documentation**

1. Speexx shall document and prove to Customer Speexx’s compliance with the obligations agreed upon in this annex by appropriate measures.
2. Where, in individual cases, audits and inspections by the Customer or an auditor appointed by the Customer are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Speexx’s operations, upon prior notice, and observing an appropriate notice period. Speexx may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Speexx shall be entitled to rejecting auditors which are competitors of Speexx.

The Customer hereby consents to the appointment of an independent external auditor by Speexx, provided that Speexx provides a copy of the audit report to the Customer.

Speexx’s time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.

1. Where a data protection supervisory authority or another supervisory authority with statutory competence for the Customer conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

**§ 7 Subcontractors (further processors on behalf of the Customer)**

1. Speexx shall use subcontractors as further processors on behalf of the Customer only where approved in advance by the Customer.
2. A subcontractor relationship shall be subject to such consent of Speexx commissioning further supplier or subcontractors with the performance agreed upon in the Customer Agreement, in whole or in part. Speexx shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.

Speexx will conduct the performance agreed upon, or the parts of the performance identified below, using the subcontractors enumerated below:

|  |  |
| --- | --- |
| Name and address of subcontractor | Description of affected parts of performance |
| INGATE/Equinix  Neue Hopfenpost  Munich, Germany | Server housing of Speexx’s own servers |

Speexx shall obtain the Customer’s consent prior to the use of new or the replacement of existing subcontractors. The Customer shall be entitled to withholding consent only for material reasons related to statutory data protection regulations.

1. Where Speexx commissions subcontractors, Speexx shall be responsible for ensuring that Speexx’s obligations on data protection resulting from the Customer Agreement and this annex are valid and binding upon subcontractor.

**§ 8 Obligations to inform, mandatory written form, choice of law**

1. Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Speexx’s control, Speexx shall notify the Customer of such action without undue delay. Speexx shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in the Customer’s sole property and area of responsibility, that data is at the Customer’s sole disposition, and that the Customer is the responsible body in the sense of the GDPR.
2. No modification of this annex and/or any of its components – including, but not limited to, Speexx’s representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.
3. In case of any conflict, the Customer Agreement regulations shall take precedence over the regulations of the annex. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.
4. This annex is subject to the laws of Germany.

**§ 9 Liability and damages**

1. The regulations on the parties’ liability contained in the Customer Agreement shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Customer** |  |  | **Speexx** |  |
| Authorised Signature: |  |  | Authorised Signature: | http://files-eu.clickdimensions.com/speexxcom-aknfj/files/speexx-test-3.jpg |
| Print Name: |  |  | Print Name: | Andreas Urban |
| Title: |  |  | Title: | Director Global Services |
| Date: |  |  | Date: | 23 May 2018 |

**Technical and Organisational Measures**

Speexx shall implement and maintain the following technical and organizational security measures (TOM) for the processing of personal data on behalf of the Customer in accordance with Article 28 of the EU General Data Protection Regulation.

These TOM apply to subcontractors who may come into contact with personal or other data of the contracting authority.

**1.** **Physical Access Controls:** Speexx shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, or to prevent unauthorized persons from gaining access to Data.

Measures implemented:

* Physical access controls based on the ISO 27001 standard.
* Speexx servers storing Data are hosted at data centre facilities in Germany which follow industry best-practices.
* On-site Security includes a secured perimeter with multi-level security zones and physical locks.
* Access control systems (smart cards, multifactor identification with biometric access control).
* Security personnel at entrances.
* Right to access generally limited to authorized Speexx personnel, security personnel, and qualified third parties under the supervision of authorized Speexx personnel.
* List of authorized people that may access data centres are maintained by Speexx and require management approval prior to access.
* Surveillance systems (alarm system, door prop alarm, motion detectors, 24x7 manned security, CCTV video surveillance).
* Lockable cabinets (servers, storage media).
* Glass break sensors.
* Visitor logbook (time and purpose of entry, time of exit).
* Denial of access triggers notification, investigation.
* All systems and networked devices are constantly monitored by Speexx.

**2.** **System Access Controls:** Speexx shall take reasonable measures to prevent Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

Measures implemented:

* Database security controls restrict access; controlled and audited by internal and external auditors chosen by Speexx.
* Access rights based on job duties and utilizing least privilege.
* Approval process for access rights; periodic reviews and audits conducted by Speexx as well as third party auditors contracted by Speexx.
* Third-Party penetration testing.
* Intrusion Detection and/or Prevention Systems which includes 24/7 monitoring.
* Password policy.
* Automatic blocking of access.
* Failed log-ons are logged by Speexx’s security infrastructure.

**3.** **Data Access Controls:** Speexx shall take reasonable measures to provide that Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Data to which they have privilege of access; and, that Data cannot be read, copied, modified or removed without authorization in the course of processing.

Measures implemented:

* Access rights based on job duties and utilizing least privilege and signing of confidentiality agreements and Non-Disclosure and Confidentiality Agreements by all employees according to Article 53 GDPR.
* Approval process for access rights; periodical reviews and audits.
* Anti-virus and redundant firewalls, security HTTPS transport over public networks by default, regular audits, and network intrusion detection/prevention technologies (IDS and/or IPS).
* Network Vulnerability Scanning, Third-Party Penetration Tests, Security Incident Event Management, Intrusion Detection and/or Prevention, Threat Intelligence Program and DDoS Mitigation.
* Secure and certified disposal of data and storage media.

**4.** **Transmission Controls:** Speexx shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Data by means of data transmission facilities is envisaged so Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

Measures implemented:

* Logging of access and activity and retention of such logs to facilitate forensic investigations.
* Prohibition to use private devices (e.g. USB devices) for storage of Data.
* Security HTTPS transport over public networks by default.

**5.** **Input Controls:** Speexx shall take reasonable measures to provide that it is possible to check and establish whether and by whom Data has been entered into data processing systems, modified or removed.

Measures implemented:

* Access rights based on job duties and utilizing least privilege.
* Approval process for access rights; periodical reviews and audits.

**6.** **Job Controls**

Speexx shall take reasonable measures to ensure that Service Data is processed in accordance with Data Processor’s instructions.

Measures implemented:

* Access to the Speexx system infrastructure is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by a small group of administrators. Employees with privileged access to the Speexx system infrastructure are required to use multiple factors of authentication.
* Security Training for employees to limit exposure to OWASP Top 10 security flaws for the Speexx application.
* All new hires are carefully selected through the hiring process and required to sign Non-Disclosure and Confidentiality Agreements according to Article 53 GDPR.
* Diligently selecting sub-processors and other service providers.
* Documenting selection procedures (privacy and security policies, audit reports, certifications).
* Standardized policies and procedures (including clear segregation of responsibilities where staffing levels allow) documented in a central knowledge base.

**7. Availability Controls (Data Backup:** Back-ups of the databases are taken on a regular basis, are secured, and encrypted to ensure that Data is protected against accidental destruction or loss when hosted by Speexx.

Measures implemented:

* Redundant circuits with separate utility feeds (where geographically available) and backup generators.
* Co-location facilities are powered by redundant power, each with UPS and backup generators.
* Air-conditioning, temperature and humidity controls (monitored 24x7).
* Disaster-resistant housing (smoke detection, fire alarm, fire suppression, water detection, raised flooring, protection against severe weather conditions, pest repellent system).
* Electrical equipment monitored and logged, 24x7 support.
* Daily backup procedures.
* Disaster recovery plan.
* Routinely test-running data recovery.
* Anti-virus/firewall systems.

**8.** **Logical Separation:** Data from different Customers is logically segregated on Speexx’s systems to ensure that Data that is collected for different purposes may be Processed separately.

Measures implemented:

* Data from different customers is logically segregated from one another.
* Co-location cage space is physically and logically separated from other co-location data centre customers.
* Data used in test environments will be protected in a manner commensurate with live production environments
* Detailed management of access rights (e.g. role-based).
* Separate environments. Testing and staging environments are logically separated from the production environment.  No actual Data is used in the development or test environments.