Agreement on order processing within the meaning of Art. 28 (3) of the General Data Protection Regulation (GDPR)

between

____

Client name

____

Client street

____

Client postcode, location

- hereinafter referred to as the **"Client"** -

and

heinekingmedia GmbH
Hamburger Allee 2-4
30161 Hanover

- hereinafter referred to as the **"Contractor"** -

- The Client and Contractor are hereinafter referred to individually as "**Party**" and together as "**Parties**" -

Preamble

This agreement on order processing within the meaning of Art. 28 (3) GDPR (hereinafter referred to as the "Agreement") specifies the obligations of the Parties with respect to data protection that arise when using schul.cloud. It applies to all activities whereby employees of the Contractor or those contracted by the Contractor process the personal data (hereinafter referred to as "data") of the Client.

1 Object, duration and specification of the data processing

(1) The Contractor shall process personal data on behalf of the Client. The object of the contract and the nature and purpose of the processing are specified in **Appendix 1**.

(2) The duration of this agreement will be determined by the term of the order form, provided that the provisions of this agreement do not entail any additional obligations.

§ 2 Responsibility, the Client's authority to issue instructions

(1) Within the framework of this agreement, the Client is solely responsible for complying with the statutory provisions of the data protection act, in particular for the lawfulness of the data transfer to the Contractor as well as for the lawfulness of the data processing ("data controller" within the meaning of Art. 4 (7) GDPR).

(2) The instructions of the Client shall be initially determined in the context of placing the order and can then be changed, supplemented or replaced by the Client in written form or in an electronic format (text form) to the office designated by the Contractor via individual instructions (individual instruction). Instructions that are not provided in the context of placing the order will be treated as an application for a change in performance; the Parties will consult on the change of performance and its commercial effects and will specify it in a written amendment agreement. The Client shall set a reasonable deadline for the Contractor to implement the instructions. Verbal instructions must be confirmed immediately in writing or in text form.

(3) The Contractor and the Client shall appoint in writing or in text form a contact person who is authorised to give (individual) instructions or to accept (individual) instructions in connection with the contractual data processing.

When changing the contact person responsible or in case of permanent hindrance of a responsible contact person, this must be communicated immediately in writing or in text form by the respective Contract Partner with appointment of a representative.

(4) There is no substantive statutory inspection obligation on the part of the Contractor with regard to instructions issued by the Client. However, if the Contractor considers that the Client's instructions violate applicable laws, it shall inform the Client immediately. The Contractor may suspend implementation of the instructions until they have been confirmed or amended by the Client. Any additional expenses incurred by the Contractor shall be borne by the Client. The Client bears the sole responsibility for the decision it has made.

§ 3 Obligations of the Contractor

(1) The Contractor may process the data of data subjects only within the scope of the order and the Client's instructions.

(2) The Contractor shall, within its area of responsibility, structure the internal organisation so that it meets the specific requirements of data protection. The Contractor will take technical and organisational measures to adequately protect the data of the Client, which meet the requirements of the General Data Protection Regulation (Art. 32 of the GDPR). Further regulations are contained in § 5 of this agreement.

(3) The Contractor shall inform the Customer immediately if it becomes aware of any breaches of the Client's data protection. In this case, the Contractor may, intermittently and at its own discretion, take measures within its area of responsibility to protect the Client's data and to mitigate possible adverse consequences. The Contractor shall inform the Client of any measures it has taken as promptly as possible.

(4) The Contractor warrants that the employees involved in processing the Client's data and other persons working for the Contractor shall not process the data other than instructed. Furthermore, the Contractor warrants that the persons authorised to process the data have been committed to confidentiality or are subject to an appropriate legally binding non-disclosure obligation. The confidentiality/non-disclosure obligation shall continue to apply even after termination of the order.

(5) The Contractor warrants compliance with the requirements for the written appointment of a data protection officer and shall inform the Client of the contact data on request. If the Contractor is not legally obliged to appoint a data protection officer, it shall inform the Client of the contact person for data protection issues arising under this agreement.

(6) At the request of the Client, the Contractor shall assist the Client within the scope of what is reasonable in

a) compliance with the Client's duties as regulated in Art. 32 to 36 GDPR;

b) the fulfilment of inquiries and claims of data subjects pursuant to chapter III of the GDPR.

The Contractor may require reasonable compensation and reimbursement of expenses for such assistance, unless this is based on the Contractor culpably breaching this agreement or applicable data protection law.

(7) In the event of a claim against the Client by a data subject, with regard to any claims under Art. 82 of the GDPR, the Contractor undertakes, within its means, to support the Client in defending the claim.

§ 4 Obligations of the Client

(1) The Client must inform the Contractor immediately and in full if errors or irregularities in the results of the order become apparent with regard to data protection regulations.

(2) The Client is responsible for fulfilment of the duties regulated in Art. 33 to 36 of the GDPR.

(3) The Client will provide the Contractor with all information required by the Contractor for keeping the directory pursuant to Art. 30 (2) GDPR. (2) GDPR.

(4) In the event of a claim against the Contractor by a data subject, with regard to any claims under Art. 82 of the GDPR, the Client undertakes, within its means, to support the Contractor in defending the claim.

(5) The Client shall inform the Contractor of the contact person for data protection issues arising under this agreement.

(6) The Client must decide on the storage, publication or deletion of the data of the Client after termination of this agreement (see § 9 of this agreement) within a reasonable period set by the Contractor. If the Contractor does not reach a decision within this period, the Contractor is entitled to delete this data, insofar as the Contractor is not subject to any legal obligations to retain this data.

§ 5 Technical and organisational measures

(1) The Contractor will, within its area of responsibility, take technical and organisational measures to adequately protect the Client's data, which will ensure the long-term reliability, integrity, availability, and resilience of the systems and services associated with such order processing, as well as the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident. The technical and organisational measures taken by the Contractor are set out in **Appendix 2** (hereinafter referred to as "TOMs").

(2) The Client is responsible for evaluation and assessment of the effectiveness of the TOMs. If these are not sufficient from the Client's perspective, the Parties shall agree on corresponding changes and their commercial effects and implement them on the basis of a corresponding written amendment agreement.

(3) The TOMs are subject to technical progress and further development. In that regard, the Contractor is permitted to implement adequate alternative measures. In so doing, the security level must not fall below that of the previously agreed measures. Significant changes must be documented.

(4) The Contractor has established a procedure to periodically review the effectiveness of technical and organisational measures to ensure the security of the processing.

§6 Correction, restriction, and deletion of data

(1) The Contractor may not, on its own initiative, correct, delete, or restrict the processing of data processed for the Client; this may only be done when instructed in writing by the Client.

(2) If a data subject approaches the Contractor with claims for correction, deletion or information, the Contractor shall refer the data subject to the Client, provided that an allocation of the data subject's request to the Client is possible according to the data of the data subject. The Contractor shall support the Client within its means and upon instruction, to the extent agreed upon. The Contractor shall not be liable if the Client does not respond to the request of the data subject, does not respond correctly, or does not respond in due time.

§ 7 Verification options, inspection rights of the Client

(1) The Contractor shall demonstrate to the Client compliance with the obligations laid down in this agreement. Verification of such measures, which not only concern the specific order, can be provided by

a) compliance with approved rules of conduct referred to in Art. 40 GDPR;

b) certification according to an approved certification procedure according to Art. 42 GDPR;

c) up-to-date certificates, reports, or report extracts prepared by independent bodies (e.g. auditors, data protection officers, IT security department, privacy auditors, quality auditors);

d) an appropriate certification with an IT security or data protection audit (e.g., pursuant to BSI-basic protection).

(2) If, in individual cases, data protection inspections or reviews are required by the Client or an independent external auditor commissioned by the latter, whose name is communicated to the Contractor in good time in advance, they will be undertaken in the presence of an employee of the Contractor during normal business hours as well as without interruption of the operation at the place of business of the Contractor after notification, taking into account a reasonable lead time. The Contractor may make the auditors subject to signing an appropriate declaration of confidentiality regarding the data of other customers and the technical and organisational measures that have been established.

(3)

(3) Upon request, the Contractor will provide the Client with all information necessary for carrying out a comprehensive inspection within a reasonable period of time.

(4) The Client shall provide the Contractor with a copy of the full audit report in electronic form. In particular, the Contractor may entrust the audit report to its subcontractors.

§ 8 Subcontractors (other contract processors)

(1) The use of subcontractors as further order processors is only permitted if the Client has previously agreed to it.

(2) A subcontractor relationship requiring approval shall exist if the Contractor commissions further contractors to perform all or part of the agreed service. The Contractor shall enter into agreements with such third parties to the extent necessary to ensure appropriate data protection and information security measures.

(3) The Client hereby agrees that the Contractor will employ the subcontractors listed in **Appendix 3**. The Contractor shall inform the Client before further employment or replacement of subcontractors.

The Client may object to the replacement within a reasonable period - for good cause - in writing or in text form. Consent shall be deemed as given if the Client does not object within the deadline.

(4) Should the Contractor place orders with subcontractors, then the Contractor shall transfer its obligations under this agreement to the subcontractor.

§ 9 Deletions and return of data

§ 9 Deletions and return of data

(1) Upon termination of this agreement, the Contractor shall, if technically possible and requested by the Client in accordance with § 4 (6) of this agreement, provide the Client's data. If required, electronically stored data can either be issued in a commercially available format on data carriers or transmitted as encrypted online to the Client.

(2) The Contractor will delete all the Client's electronically stored data, of which the Client does not wish to release pursuant to the above paragraph 1 or for which release is not technically possible. The Contractor will confirm the deletion on request in writing.

(3) The Client's data that is not stored in electronic form (e.g. data on CDs, paper-based documents) and which the Client does not wish to release pursuant to paragraph 1 above, shall be destroyed by the Contractor in accordance with data protection.

(4) The obligation to release or delete pursuant to this § 9 does not exist if the Contractor is legally obliged to retain or otherwise store this data.

(5) If the Client wishes to retain his data beyond the end of the contract, this shall require a separate agreement between the Parties. The Parties shall agree on the corresponding services and commercial effects and will define them in a written amendment agreement.

§10 Concluding provisions

(1) If the Client's data is endangered by seizure or confiscation, due to an insolvency or settlement procedure or due to other events or measures of third parties, the Contractor will notify the Client without delay, unless the relevant law prohibits such notification because of an important public interest. The Contractor shall immediately inform the third party that the Client has exclusive authority over and ownership of the data as "data controller" within the meaning of the GDPR.

(2) Amendments and additions to this agreement and all of its components must be undertaken in writing. This also applies to the waiver of this written form requirement.

(3) Should a provision of this agreement be or become ineffective or should this agreement contain a loophole, the validity of the agreement shall otherwise not be affected. The ineffective provision shall be replaced by the legally permissible provision which comes closest to commercial intentions of the Parties when the agreement was concluded. A loophole should be replaced by a provision that corresponds to what the Parties would have agreed in the sense and purpose of the agreement, taking into account all circumstances, if they had been aware of the existence of the loophole.

(4) German law shall apply.

(5) The place of jurisdiction for all disputes arising from or in connection with this agreement is Hanover, insofar as the Contractual Partner is a merchant within the meaning of the German Commercial Code, a legal entity under public law, or a special fund under public law. However, in this case, the Contractor is also entitled to bring an action before the court having jurisdiction for the Client.

Appendix 1

Object and specification of the data processing

I. Object of the data processing

The Contractor shall provide the Client with the learning and communication platform schul.cloud. schul.cloud is a communication platform for schools and educational institutions for organising and facilitating communication within the day-to-day life of schools. schul.cloud is available as a browser web interface, as a desktop client for Windows and Mac, and as a mobile app for iOS and Android. The integrated real-time messenger enables direct communication via the platform, and its integrated file storage option can be used by any user as their own cloud. Each user creates their own account with the appropriate permission level, which authorises use of the platform.

II. The nature and purpose of data processing

When using schul.cloud, personal data is processed for the purpose of clear communication. Each user receives a separate account in the schul.cloud platform, which includes the user's first and last name in plain text. The first and last names are used to assign the users within the framework of the platform in order to enable communication with the desired conversation partner. Each user also receives a corresponding user role. This is needed to control permissions within the platform. Each user registers their own account and enters an email address and account password as login information, which are used to log in to schul.cloud. This email address is not visible to other users within the platform (except for administrators). Only the user can see and change their email address on the platform.

III. Types of personal data

Each user is created in the schul.cloud platform with specific user attributes. The following types of personal data are processed in this respect:

- Last name
- Possibly a title or abbreviation
- First name
- Entry date
- Possibly an exit date
- Email address
- Possibly a photo
- Communication data: as soon as a user interacts or communicates on the platform, the communication data required to use the platform will be collected. This includes information about users' activity on the platform (e.g. information about membership in a channel), which will be stored in the system. Using the site would not be possible without processing this data. This communication data also includes the entry and exit dates.

IV. Categories of data subjects

The categories of data subjects using schul.cloud are:

- Teachers/school management/school staff
- Students
- Parents (optional)

Appendix 2
Technical and organisational measures

I. Confidentiality (Art. 32 (1) (b) of the GDPR)

Pseudonymisation
Pseudonymisation of data can only be undertaken by prior agreement.

Encryption
All systems are installed, configured, and administered using an encryption concept, or based on the customer's specific provision. This concerns both the transport encryption as well as the encryption of data carriers, directories, and files.

Data carrier shipment
Physical data carriers are usually not shipped, and if required by the customer, this will be undertaken using effective encryption techniques

Multi-factor authentication
Access to the data processing systems is only possible after successful authentication based on at least two factors of different types (e.g. biometric feature and PIN).

Access logging
Any access to secure areas where data processing systems are located is automatically logged and can therefore be tracked.

Video surveillance
Secure areas containing data processing systems are continuously monitored by video cameras. These recordings are saved and retained for a reasonable time period.

Locked racks
Racks containing data processing systems are locked. The keys are managed centrally.

Emergency doors
Secure areas may only be entered via the designated entrances. Emergency doors cannot be used as an entrance from the outside. Opening these emergency doors triggers an alarm.

Authorisation requirement
Admission or access to the secure areas or systems is subject to a formalised authorisation process.

Cleaning and maintenance work

No unaccompanied maintenance or cleaning work is undertaken by unauthorised persons in secure areas.

Passwords

Access to data processing systems is only possible after prior authentication based on usernames and passwords. The minimum requirements for password length and complexity as well as the handling of passwords are defined in a guideline and are supported by the system. Passwords are generated with random number generators. Passwords are transmitted as encrypted in the log in process.

Access logging

Every log in to a data processing system is logged. The logs are protected against change and will be retained for a reasonable period of time.

Classification

A policy governs the classification of data types, such as personal data and related provisions.

Client separation

Data processing systems of different Clients are physically or logically separated from each other so that unauthorised access by each other is excluded.

Mobile data carriers

Personal data will not be stored for internal use on mobile data carriers, such as USB flash drives or DVDs.

Segregation of duties

Administration of the data processing systems and their infrastructure involves various employees, whose responsibilities and authorisations are regulated as per a role concept.

Periodic review

As part of internal audits, access authorisations for data processing systems are regularly inspected and reviewed with respect to their legality.

Revocation of permissions

When terminating or changing the employment of employees, access permissions that are no longer required will be revoked.

Screen lock

Employees' workstations are configured to enable password-protected screen lock after a time interval has expired.

II. Integrity (Art. 32 (1) (b) of the GDPR)

Authorisation requirement
Access permissions to the data processing systems are subject to a formalised approval process.

Logging
Every system access is logged. The logs are protected against change and will be retained for a reasonable period of time.

III. Availability and reliability (Art. 32 (1) (b) of the GDPR)

Fire protection
Data centres are equipped with adequate systems for detecting fires and with alarm systems. Extinguishing systems are available in critical secure areas. Secure areas are regularly checked for avoidable fire loads.

Power supply
The data centres have an uninterruptible power supply (UPS) system that ensures continued operation of the data processing systems in the event of power failure. Critical secure areas are also equipped with an emergency power system (EPS), which ensures independent power supply even over longer periods of time.

Air conditioning
The appropriate temperature and humidity in the data centres is ensured via redundant air conditioning units.

Network connection
The agreed connection of data processing systems to agreed networks is undertaken via redundant lines from various providers.

Data backup
Customer systems are backed up pursuant to the agreements in the main contract. Internal systems are backed pursuant to a backup concept.

Security systems
Critical parts of the infrastructure are protected by appropriate systems to prevent or reduce the impact of attacks or disruptions (security systems).

Periodic review
Security systems are regularly reviewed for adequacy and effectiveness.

Emergency plans
There are emergency plans for emergency preparedness and emergency treatment for each site.

Regular testing

All emergency concepts will be tested regularly and the results documented.

IV. Regular review, assessment, and evaluation of data protection

General data processing contract

If a subcontractor is commissioned, rights and obligations shall be regulated in a general data processing contract.

Monitoring

All contractors of MIVITEC GmbH involved in data protection are regularly audited to check for compliance with the agreed measures.

Audit

All data protection-relevant processes and documents are regularly audited to determine if they are up to date and effective.

V. Other measures

Data protection officer

MIVITEC GmbH has appointed a competent external data protection officer, whose name and contact information can be found in the procedure directory.

Data protection concept

The handling of personal data is regulated in a data protection concept that is binding for all employees.

Declaration of commitment

All employees are bound by data privacy laws in the sense of data protection legislation.

Training

All employees are regularly trained by a competent data protection expert in the handling of personal data.

Periodic review

All data protection measures are regularly reviewed as part of internal audits.

Appendix 3

Subcontractors

Name and registered office of the subcontractor	Activity undertaken by the subcontractor
MIVITEC GmbH, Wamslerstr. 4, 81829 Munich	Provision (hosting) of the schul.cloud platform in the high security data centre

This letter was created automatically and is valid without a signature.