Data Processing Agreement

pursuant to Art. 28 (3) GDPR · Skool Extensions CRM Cloud Sync

Version 1.0
As of: 27 May 2026
skool-extensions.com/dpa

Controller

The user of the browser extension "Skool Extensions" who activates the CRM feature and collects and processes CRM data about Skool members of his/her Skool community.

Hereinafter: "Controller".

Processor

Marco Hanczuch — Skool Extensions
Oderstr. 56a
14513 Teltow
Germany
E-mail: mail@flowdesk.de
Web: skool-extensions.com

Hereinafter: "Processor".

— hereinafter jointly referred to as the "Parties" —

Entry into force: This Agreement is concluded between the Parties when the Controller, upon first activating the CRM Cloud Sync feature in the "Skool Extensions" browser extension, confirms the consent statement ("Accept DPA"). The time of acceptance is logged electronically.

Preamble

The Controller uses the "Skool Extensions" browser extension provided by the Processor, including its CRM Cloud Sync feature, in order to record and maintain data about members of the communities he/she operates or administrates on the platform *skool.com*, and to synchronise this data across multiple browsers or devices. In the course of providing this feature, the Processor receives access to personal data for the processing of which the Controller is responsible within the meaning of the GDPR. This Agreement specifies the data protection obligations of the Parties pursuant to Art. 28 GDPR.

§ 1 Subject Matter and Duration of Processing

(1) Subject matter

The subject matter of the engagement is the encrypted storage, synchronisation and provisioning — carried out within the CRM Cloud Sync feature of the "Skool Extensions" extension — of CRM data records that the Controller collects about Skool community members (in particular contact data, notes, tags and pipeline status), as well as the delivery of such records to other browsers/devices of the same Controller and, where activated, to further administrators of the relevant Skool community.

(2) Duration

This Agreement is concluded for an indefinite period and ends upon deactivation of the CRM Cloud Sync feature by the Controller, uninstallation of the extension, or revocation of the DPA. Ordinary termination is possible at any time without notice. The right to extraordinary termination remains unaffected.

§ 2 Nature and Purpose of Processing, Categories of Data Subjects and Data

(1) Nature and purpose

The processing comprises the collection, storage, encryption, transmission, synchronisation, pseudonymisation, deletion and destruction of personal data exclusively for the purpose of providing the CRM Cloud Sync feature. Processing for any other purpose — in particular for advertising, profiling or AI training — does not take place.

(2) Categories of data subjects

- Members of Skool communities that the Controller operates or administrates/moderates.
- Optionally: further persons listed in the community (e.g. applicants, contacts) whom the Controller manually adds as a CRM profile.

(3) Categories of personal data

- **Master data:** Skool member ID, publicly visible display name, avatar URL.
- **CRM data entered by the Controller:** phone number, e-mail address (if added manually), location/company/language, notes, tags, pipeline stage, deal value, follow-up date, custom fields, links.
- **Activity metadata:** timestamp of the last profile visit, timestamp of the last data change, audit-log entries (which admin changed which field at what time).
- **Technical metadata:** workspace ID, version counters for last-write-wins merge.

Special categories of personal data (Art. 9 GDPR) are not subject of the processing; the Controller undertakes not to enter such data into the CRM.

§ 3 Obligations of the Processor

1. The Processor shall process personal data only within the scope of the agreements concluded and on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject (Art. 28 (3) lit. a GDPR).
2. The Processor shall not use the data for any other purpose and in particular reserves no right to use the data for its own purposes (e.g. profiling, AI training, advertising).
3. The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality (Art. 28 (3) lit. b GDPR).
4. The Processor shall implement the technical and organisational measures set out in § 4 (Art. 32 GDPR).
5. The Processor shall, to the extent possible, assist the Controller by appropriate technical and organisational measures in fulfilling the obligations under Art. 32 to 36 GDPR and in responding to requests by data subjects (Art. 12 et seq. GDPR).
6. The Processor shall inform the Controller without undue delay if, in its opinion, an instruction infringes the GDPR or other data protection provisions.
7. The Processor shall not transfer data to third countries unless expressly provided for in this Agreement — in particular in Annex 2.

§ 4 Technical and Organisational Measures (TOM)

The Processor shall implement the technical and organisational measures within the meaning of Art. 32 GDPR set out in **Annex 1** and adapt them continuously to the state of the art. Substantial changes shall be documented; a reduction of the level of protection is not permitted.

§ 5 Sub-Processors

1. The Controller grants the Processor the general authorisation listed in **Annex 2** to engage the sub-processors named therein (Art. 28 (2) GDPR).
2. The Processor shall inform the Controller of any intended changes regarding the addition or replacement of other sub-processors. The Controller has the right to object to such changes.
3. The Processor shall impose on each sub-processor — by way of a contract or another legal instrument — the same data protection obligations as set out in this Agreement (Art. 28 (4) GDPR).

§ 6 Rights of Data Subjects

The Processor shall assist the Controller by appropriate technical and organisational measures in fulfilling its obligation to respond to requests by data subjects for the exercise of their rights to information, rectification, erasure, restriction of processing, data portability, objection, and withdrawal of granted consent (Art. 12 to 22, 32 GDPR). If a data subject addresses such a request directly to the Processor, the Processor shall forward the request to the Controller without undue delay.

§ 7 Notification Obligations for Data Breaches

1. The Processor shall notify the Controller without undue delay, and in any event within **48 hours** of becoming aware, of any breach of the protection of personal data occurring in connection with this processing engagement.
2. The notification shall include, to the extent known at the time of reporting: a description of the nature of the breach; categories and approximate number of data subjects and data records affected; measures taken or proposed to mitigate the breach; likely consequences; contact details of the point of contact (Art. 33 (3) GDPR).
3. Obligations to notify the supervisory authority and the affected data subjects pursuant to Art. 33, 34 GDPR remain the responsibility of the Controller.

§ 8 Audit Rights of the Controller

1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.
2. Audits shall be carried out in the form of written self-disclosures by the Processor and, where necessary, by on-site inspections following prior notice with reasonable lead time, during normal business hours and without disrupting operations. The cost of on-site inspections shall be borne by the Controller.

3. Current certificates, reports or report extracts from independent bodies (e.g. ISO 27001 certificates of sub-processors) shall be provided on request.

§ 9 Deletion and Return after Termination

1. The Controller may export his/her CRM data at any time from within the extension (“Export data” in the extension settings) and may mark individual records or the entire workspace for deletion.
2. Upon termination of this Agreement (e.g. through revocation of the DPA, deactivation of CRM Cloud Sync, or uninstallation of the extension), the Processor shall delete all personal data made available to it within the scope of this Agreement within at most **30 days**, unless storage is required by a legal provision.
3. Backups containing personal data are overwritten automatically within the regular backup rotation cycle of up to 35 days.
4. Deletion shall be confirmed in writing (including by e-mail) upon request.

§ 10 Liability

For damage caused to a data subject by processing not in compliance with the GDPR, the Controller and the Processor are liable in accordance with Art. 82 GDPR. In the internal relationship between the Parties, each Party shall bear damage to the extent it is responsible for it.

§ 11 Final Provisions

1. Should any provision of this Agreement be or become invalid, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced by a valid provision that most closely reflects the economic intention of the Parties.
2. Amendments and supplements to this Agreement must be made in text form (including electronically).
3. This Agreement is governed by the laws of the Federal Republic of Germany, excluding the UN Sales Convention.
4. Place of jurisdiction shall be, to the extent legally permissible, the registered seat of the Processor.
5. In the event of conflicts between provisions of this Agreement and any other agreements between the Parties, the provisions of this Agreement shall prevail.

Annex 1 — Technical and Organisational Measures (TOM) pursuant to Art. 32 GDPR

1. Confidentiality (Art. 32 (1) lit. b GDPR)

1.1 Physical access control

- Server hardware is located exclusively in certified data centres operated by the sub-processors engaged (see Annex 2). These provide turnstile entry, video surveillance, biometric and multi-stage access control, 24/7 on-site security and logged visitor access.
- The Processor itself has no physical access to the server hardware.

1.2 System access control

- Administrative access to the backend is secured exclusively via personal accounts with strong passwords (minimum 16 characters, generated by a password manager) and, where supported, two-factor authentication.
- End-user access to CRM data is granted exclusively through the browser extension; authentication against the backend is based on a signed bearer token issued during initial pairing with the Skool account.
- Failed authentication attempts are logged; suspicious patterns lead to automatic lockout.

1.3 Data access control

- Applications access the database only with the minimum privileges required for the respective service (least privilege).
- CRM records are workspace-scoped: a user can access only records of those workspaces in which he/she is owner or admin of the associated Skool community.
- The backend API enforces this separation server-side on every individual request.

1.4 Separation control

- Data of different Controllers is logically separated in the database by unique workspace identifiers.
- Test, staging and production environments are strictly separated.
- No real personal data is processed in non-production environments.

1.5 Pseudonymisation and encryption

- All CRM data fields are encrypted server-side with **AES-256-GCM** before storage.
- Transmission between browser extension and backend takes place exclusively via TLS 1.2 or higher.
- Skool member IDs are used as opaque identifiers; re-identification without access to the Controller's Skool account is not possible.

2. Integrity (Art. 32 (1) lit. b GDPR)

- **Transmission control:** Data transfers are exclusively TLS-encrypted. Write operations to the backend are authenticated by a bearer token and checked for tampering before processing.
- **Input control:** All write API calls are logged with timestamp, user ID and workspace ID (audit log). Audit logs are accessible via the settings panel of the extension.

- **Versioning:** Conflicts between simultaneous write operations by multiple administrators are resolved through a last-write-wins mechanism with per-field granularity.

3. Availability and resilience (Art. 32 (1) lit. b GDPR)

- **Backup:** Automated daily backups of the database by the hosting data centre. Rotation cycle: up to 35 days. Backups are encrypted.
- **Recovery:** Restore tests are performed regularly. Recovery time objective (RTO) is typically less than 24 hours.
- **Attack protection:** Web application firewall, brute-force protection, automatic blocking of suspicious IP ranges.
- **Updates:** Server software is kept at current security level; security-relevant patches are applied promptly.

4. Procedures for regular review, assessment and evaluation (Art. 32 (1) lit. d GDPR)

- **Data protection management:** The Processor maintains a record of processing activities pursuant to Art. 30 GDPR.
- **Incident response:** The procedure for personal data breaches is documented; the notification deadlines under § 7 are established.
- **Sub-processor management:** Sub-processors are reviewed for data protection suitability prior to engagement and at least annually thereafter.
- **Data protection by design and by default (Art. 25 GDPR):** Data minimisation — only the data fields strictly necessary for the CRM function are stored. All encryption and separation mechanisms are active by default.

Annex 2 — Approved Sub-Processors

By concluding this Agreement, the Controller approves the engagement of the following sub-processors:

Sub-processor	Address	Service	Processing location
ALL-INKL.COM Neue Medien Münnich	Inh. René Münnich Hauptstraße 68 02742 Friedersdorf Germany	Web hosting and database hosting for the CRM backend (PHP, MariaDB); storage of encrypted CRM records; daily backups.	Germany (EU)
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Germany	Provision of server infrastructure (Docker containers) for auxiliary services of the extension (e.g. media conversion). CRM data is not persisted on this infrastructure.	Germany (EU)

All sub-processors listed above are established within the European Union and process data exclusively on servers within the EU. No data transfer to third countries takes place.

The Processor shall notify the Controller of changes to this list — in particular the engagement of additional or the replacement of existing sub-processors — with reasonable lead time (generally at least four weeks before the change takes effect). The Controller may object within this period. In the event of a justified objection, the Processor is entitled to terminate this Agreement with reasonable notice if an amicable solution cannot be reached.

Controller

Acceptance of this Agreement is provided electronically by confirming the consent statement ("Accept DPA") within the "Skool Extensions" browser extension. Date and time of acceptance are logged in the Processor's backend.

A handwritten signature is not required pursuant to Art. 28 (9) GDPR; the electronic format (click-wrap) is equivalent.

Processor

Marco Hanczuch · Skool Extensions

Teltow, 27 May 2026