Data Processing Agreement under Art. 28 GDPR

between the customer as controller (“Customer”) and LeanActivity GmbH, Braunstr. 5, 81545 Munich, Germany, as processor (“Provider”)

1. Subject matter and duration

(1) The Provider provides the Customer with the LeanActivity Online Game, a browser-based training game with live workshops led by the Customer's trainers and solo runs with personal codes and a certificate (“Main Agreement”), and processes personal data on the Customer's behalf.

(2) This agreement applies for the term of the Main Agreement and for as long as the Provider processes the Customer's personal data.

(3) It does not apply to the purchase of physical game kits or to on-site training. There, the Provider does not process personal data on the Customer's behalf.

2. Nature and purpose, types of data, data subjects

The nature and purpose of the processing, the types of personal data, the categories of data subjects and the retention periods are set out in Annex 1.

3. Instructions

(1) The Provider processes data only on documented instructions from the Customer. Instructions result from this agreement, the Main Agreement and the use of the game, such as starting workshops and creating codes in the trainer area; further instructions are given in text form.

(2) The Provider informs the Customer without undue delay if it considers an instruction to infringe data protection law.

(3) Processing without instructions only takes place where Union or Member State law requires it; the Provider informs the Customer beforehand where legally permitted.

4. Confidentiality

The Provider only uses persons who are committed to confidentiality or under a statutory obligation of confidentiality.

5. Security of processing

The Provider implements the technical and organisational measures under Art. 32 GDPR set out in Annex 2 and may develop them further provided the level of protection is not reduced.

6. Sub-processors

(1) The Customer approves the sub-processors listed in Annex 3.

(2) The Customer gives general authorisation for further sub-processors. The Provider announces changes at least 30 days in advance at leanactivity.com/avv and by email to the Customer's trainers. The Customer may object for good reason related to data protection; if no agreement is reached, the Customer may terminate the Main Agreement for cause.

(3) The Provider imposes the data protection obligations of this agreement on its sub-processors by contract.

(4) Transfers to third countries take place only under the conditions of Art. 44 et seq. GDPR, in particular based on an adequacy decision (including the EU-U.S. Data Privacy Framework) or the EU Standard Contractual Clauses.

7. Assistance

(1) The Provider assists the Customer in responding to data subject requests (Art. 12–22 GDPR) and forwards requests it receives directly. On the Customer's instruction, it deletes individual data early, for example the name and saved game at a code or a certificate.

(2) The Provider assists the Customer with Art. 32–36 GDPR, taking into account the information available to it.

8. Personal data breaches

The Provider notifies the Customer without undue delay, where possible within 48 hours of becoming aware, with the information under Art. 33(3) GDPR as far as available.

9. Deletion and return

(1) The Provider deletes personal data automatically when the retention periods in Annex 1 expire. The deletion runs every day.

(2) During the term of the contract, trainers can download the list of their solo codes with status (CSV) and the certificates (PDF). On request, the Provider also provides the stored personal data in a common format. The game does not store results of individual people, so there are none to return.

(3) When the Main Agreement ends, the Provider deletes the Customer's trainer accounts. The remaining data is deleted when its retention period in Annex 1 expires. Certificates already issued stay verifiable for 3 years after issue so that participants can prove their training; on the Customer's instruction, the Provider deletes them earlier. Statutory retention obligations remain unaffected. Restore points of the database expire after 30 days.

10. Evidence and audits

(1) The Provider makes available the information necessary to demonstrate compliance with Art. 28 GDPR.

(2) Audits, including by an auditor bound to confidentiality and commissioned by the Customer, are possible by arrangement with reasonable notice during normal business hours. Evidence may also be provided through current audit reports or certifications of the sub-processors.

11. Liability

Art. 82 GDPR applies; otherwise the provisions of the Main Agreement apply.

12. Final provisions

(1) In matters of data protection, this agreement prevails over the Main Agreement.

(2) Amendments require text form.

(3) German law applies.

(4) If a provision is invalid, the remainder of the agreement stays effective.

Annex 1: Subject matter of the processing

Purpose: Provision and operation of the LeanActivity Online Game: running live workshops (lobbies) led by the Customer's trainers, solo runs with personal codes, issuing and verifying certificates, administering trainer accounts and licences, and sending account emails.

Types of personal data and retention periods:

GROUP	DATA	PURPOSE	DELETED
Trainers	Name, email address, language for emails, password (stored only as a salted hash), sign-in sessions, the codes they created	Sign-in, licence administration, account emails (invitation, new password, “password changed”)	With the end of the customer's contract. Sessions after 30 days without use, at the latest after 90 days
Workshop participants	Display name (a nickname is fine), look of the avatar, actions in the game, team points during the workshop	Running the live workshop	20 minutes after the last connection, 2 hours after the final round, at the latest 12 hours after the start
Solo participants	Name (for the certificate), saved game to continue on another device, start and finish time	Solo training, continuing a run, certificate	30 days after the run ends (finished, or play time of 30 days over)
Certificates	Name, training, company, date, verification number. No points	Proof of participation, verification of authenticity by third parties	3 years after issue (test certificates after 7 days)
Lobby log	Time, workshop code, customer, trainer, number of seats, number of players who joined, last phase. No participant names, no points	Licence use, support	400 days after the workshop was created
Technical data	IP address, email address and user ID of sign-in attempts, only as short-lived rate-limit counters in memory; browser and connection features checked by the bot check (Cloudflare Turnstile), then a pass cookie; Cloudflare's technical logs	Security, protection against guessing of passwords and codes and against bots	Counters when their time window ends, at the latest after 60 minutes, never stored. Pass cookie after 2 hours

Categories of data subjects: The Customer's employees and other participants of its trainings, and its trainers. Special categories of personal data (Art. 9 GDPR) are not intended.

Not processed: Assessments of the performance of individual people for the Customer (no points per person for trainers or the Provider, no export of results), tracking, profiling.

Annex 2: Technical and organisational measures

- **Confidentiality:** Trainer accounts only by invitation; passwords stored as salted PBKDF2-SHA256 hashes; sessions as HttpOnly cookies with expiry; one-time links; trainers only see their own organisation and their own codes; participants without an account; no points of individual people for trainers or the Provider.
- **Integrity:** Encryption in transit (TLS); server-side validation of all input; Content Security Policy; no third-party scripts apart from the bot check.
- **Availability and resilience:** Operation on Cloudflare's redundant infrastructure; restore points of the database for 30 days; rate limits and bot check; updates only when no workshop is running.
- **Procedures for regular review:** Automated tests, including the retention periods; review of these measures and the sub-processors at least once a year.
- **Deletion concept:** Automatic deletion every day according to the retention periods in Annex 1.

Full description: Technical and organisational measures (TOMs) at leanactivity.com/avv#toms.

Annex 3: Sub-processors

PROVIDER	PURPOSE	LOCATION
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Hosting and running the game (Workers), database (D1), live workshop sessions (Durable Objects), the daily automatic deletion, bot check (Turnstile)	Database and workshop sessions: stored and processed in the EU (Cloudflare jurisdiction “eu”). Rate-limit counters only in memory, never stored. The game itself is delivered via Cloudflare's global network
ALL-INKL.COM – Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf, Germany	Sending account emails to trainers (invitation, new password, “password changed”) from noreply@leanactivity.com	Germany

Cloudflare, Inc. is based in the USA. Transfers rely on the EU Standard Contractual Clauses in Cloudflare's Data Processing Addendum and on Cloudflare's certification under the EU-U.S. Data Privacy Framework.