Technical and organisational measures (TOMs) under Art. 32 GDPR

This description supplements Annex 2 of the data processing agreement for the LeanActivity Online Game. The terms “Provider” and “Customer” have the same meaning as in the DPA.

The Provider does not operate its own servers or data centres. The game runs with the sub-processors listed in Annex 3 of the DPA. Their physical and technical safeguards are described in their data processing agreements and evidenced by certifications and audit reports; the Provider makes them available on request.

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

- **Physical access control:** No server rooms of its own. Game, database and workshop sessions run in Cloudflare's data centres; the database and the workshop sessions are stored and processed in the EU. Account emails are sent via ALL-INKL in Germany. Physical access is secured by the operators.
- **System access control:** There is no self-registration: trainer accounts are only created by invitation. Passwords are stored only as salted PBKDF2-SHA256 hashes. Sessions are HttpOnly cookies with a limited lifetime (trainers: 30 days without use, at the latest 90 days; administrators: 12 hours without use, at the latest 7 days) and end immediately on sign-out, password change or block. Invitation and password links are one-time links (valid for 7 days and 24 hours). Rate limits slow down guessing of passwords and codes; a bot check (Cloudflare Turnstile) protects sign-in, joining and solo codes.
- **Data access control:** Roles: administrator (the Provider) and trainer (only their own organisation and their own codes). Participants have no account. Trainers and the Provider see no points of individual people. In its overview, the Provider only sees counts, such as how many people are in a lobby and which phase it is in, no names and no points.
- **Separation control:** Each live workshop runs in its own isolated session (Durable Object). Data in the database is queried per organisation.
- **Data minimisation:** From participants, the game only needs a display name (a nickname is fine) or, for a solo run with certificate, a name. Certificates carry no points. No tracking, no analytics, no advertising cookies; fonts are hosted by the game itself, and the only external script is the bot check. In the participant's browser, the game keeps the seat, the language and a saved game to continue (local storage).

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

- **Transfer control:** All connections are encrypted with TLS. There is no export of results. The list of solo codes (CSV) is only available to the trainer who created them, certificates (PDF) to the participant and the trainer. The verification page only shows name, training, company and date, and only to someone who knows the verification number.
- **Input control:** All input is validated on the server; the game state of a workshop is kept by the server, not by the players' browsers. The lobby log records when a workshop was created, by which trainer, with how many seats and players, without participant names.

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

- **Availability control:** Operation on Cloudflare's redundant global infrastructure. Rate limits and the bot check protect against overload. Before every update, an automatic check makes sure that no workshop is running.
- **Recoverability:** The database can be restored to an earlier point in time within the last 30 days. The game itself can be redeployed from source code management at any time.

4. Regular testing and evaluation (Art. 32(1)(d) GDPR)

- **Automated tests:** Automated tests check, among other things, sign-in, the roles and the retention periods before every update.
- **Review of these measures:** These TOMs and the list of sub-processors are reviewed and updated at least once a year and whenever significant changes occur.
- **Processor control:** Sub-processors are only used under a data processing agreement (Annex 3 of the DPA). Their certifications and audit reports are taken into account when selecting them and regularly afterwards.

5. Organisational measures

- **Authorised persons:** Only persons of the Provider who need it for operation, support or troubleshooting have access to customer data, and only after being bound to confidentiality.
- **Personal data breaches:** The Provider notifies the Customer of personal data breaches without undue delay, where possible within 48 hours of becoming aware (section 8 of the DPA).
- **Deletion concept:** A daily job deletes all data whose retention period has expired (Annex 1 of the DPA), in one transaction. Its log only contains the number of deleted records per type, no personal data.
- **Data subject rights:** Requests received directly by the Provider are forwarded to the Customer. On the Customer's instruction, the Provider deletes individual data early, such as the name and saved game at a code or a certificate.