# Data Processing Agreement (DPA)

Last Updated: 2026-04-16 Effective Date: 2026-04-16

## 1. Subject Matter and Scope

1.1. This Data Processing Agreement (**"DPA"**) governs the Processing of Personal Data that Genz IT Solutions GmbH (**"Provider"**, **"Processor"**) processes via the cloud services on behalf of the customer (**"Controller"**).

1.2. This DPA applies exclusively to the cloud services of the Capawesome Platform. The following are not covered:

- **Capawesome Insiders SDKs**: These are delivered via the Capawesome package registry and, after download, run entirely locally on the customer's device. No data flow to the Provider's servers occurs at runtime. Download access logs are processed by the Provider as an independent Controller (Privacy Policy).
- **Standalone open-source libraries**: Open-source libraries of the Capawesome organisation that do not communicate with the Capawesome Platform are subject solely to the applicable open-source licence.

1.3. This DPA applies uniformly to the trial period and to paid subscriptions. There are no tiered modules or tier distinctions.

## 2. Precedence

2.1. In the event of a conflict between this DPA and the Terms of Service, this DPA shall prevail insofar as the Processing of Personal Data is concerned.

## 3. Nature, Purpose and Duration of Processing

3.1. The nature, purpose and subject matter of the Processing as well as the categories of Personal Data and Data Subjects are set out in **Annex 1**.

3.2. Processing shall take place for the duration of the contractual relationship between the parties plus the deletion and retention periods set out in Section 13.

3.3. The sole purpose of the Processing is the provision of the cloud services commissioned by the Controller.

## 4. Instructions

4.1. The Provider shall process Personal Data solely on the basis of documented instructions from the Controller. This DPA and the Terms of Service constitute the initial instructions. Supplementary instructions shall be given in text form (§ 126b BGB (German Civil Code)).

4.2. The Controller is the sole Controller under data protection law for the data processed on its behalf. The Controller shall ensure that the Processing is based on a valid legal basis.

4.3. The Controller shall independently obtain and maintain all consents, notices and legal bases required under the GDPR and the TDDDG (German Telecommunications Digital Services Data Protection Act) for the collection and transmission of end-user data via Capawesome SDKs before embedding them in its applications.

4.4. The Provider shall inform the Controller without undue delay if, in the Provider's opinion, an instruction infringes applicable data protection law (Art. 28(3) sentence 3 GDPR). The Provider may suspend the Processing until the matter is resolved.

4.5. The Provider shall be entitled to refuse to carry out manifestly unlawful instructions until the Controller demonstrates their lawfulness or amends the instruction.

## 5. Confidentiality

5.1. The Provider shall ensure that all persons authorised to process Personal Data are bound by confidentiality obligations or are subject to an appropriate statutory duty of secrecy.

5.2. The confidentiality obligation shall survive the termination of the respective engagement.

## 6. Technical and Organisational Measures

6.1. Before commencing the Processing, the Provider shall implement the Technical and Organisational Measures (TOMs) described in **Annex 2** for the protection of Personal Data in accordance with Art. 32 GDPR.

6.2. Amendments to the TOMs are permissible provided the level of security documented in Annex 2 is not reduced. Material changes shall be notified to the Controller.

## 7. Sub-processors

7.1. The Controller grants the Provider a general authorisation to engage Sub-processors. The current list is available at https://capawesome.io/subprocessors and forms part of this DPA as **Annex 3**.

7.2. The Provider shall notify the Controller at least **30 days** before the planned engagement of a new or changed Sub-processor in text form.

7.3. The Controller may object to the engagement of a new or changed Sub-processor on legitimate data protection grounds within the notice period in text form. If the parties are unable to reach an amicable solution, the Controller shall have an extraordinary right of termination for the affected cloud service with a pro-rata refund. The Provider is not obligated to maintain parallel operations or to engage alternative Sub-processors.

7.4. The Provider shall contractually ensure that Sub-processors are subject to the same data protection obligations as agreed in this DPA.

7.5. **Apple and Google**: In the context of App Store Publishing, the Provider acts as an API pass-through to the Controller's own developer accounts with Apple and Google. Apple and Google are independent controllers with a direct contractual relationship with the Controller and are not Sub-processors of the Provider.

7.6. **Merchant of Record**: Polar Software Inc. and Lemon Squeezy LLC act as independent controllers in the purchase process, not as Sub-processors of the Provider.

7.7. **Ancillary services**: Routine ancillary services (cleaning, telecommunications, transport, security guarding) do not constitute Processing on behalf of the Controller within the meaning of Art. 28 GDPR, even if the service providers may incidentally have access to premises or infrastructure. The Provider shall ensure that data security is maintained in connection with such services.

## 8. International Data Transfers

8.1. Where Personal Data is transferred to Sub-processors outside the EEA, the Provider shall ensure that an adequate level of data protection is maintained.

8.2. For transfers to the USA, the Provider primarily relies on the EU-US Data Privacy Framework (DPF) for DPF-certified recipients. In addition, EU Standard Contractual Clauses (SCCs) pursuant to Implementing Decision (EU) 2021/914 (Module 3, Processor to Processor) are in place (**Annex 4**).

8.3. The Provider shall conduct a Transfer Impact Assessment for each third-country transfer and shall make the documentation available to the Controller upon request.

8.4. Supplementary addenda for transfers under the UK International Data Transfer Addendum (IDTA) and the Swiss revFADP shall be added as further annexes when there is an actual need.

## 9. Assistance with Data Subject Rights

9.1. The Provider shall assist the Controller with appropriate technical and organisational measures in fulfilling Data Subject requests (Art. 15–22 GDPR).

9.2. If the Provider receives a request directly from a Data Subject, the Provider shall forward it to the Controller without undue delay.

## 10. Personal Data Breach Notification

10.1. The Provider shall notify the Controller without undue delay and in any event no later than **48 hours** after becoming aware of a Personal Data breach within the meaning of Art. 33 GDPR.

10.2. The notification shall contain at least:

- a description of the nature of the breach, including the categories and approximate number of Data Subjects and data records affected,
- the name and contact details of a contact person for further information,
- a description of the likely consequences of the breach,
- a description of the measures taken or proposed to remedy the breach and mitigate its effects.

10.3. Where not all information is available at the same time, the information may be provided in stages, without exceeding the 48-hour deadline for the initial notification.

## 11. Assistance with DPIAs and Prior Consultation

11.1. The Provider shall provide reasonable assistance to the Controller in carrying out Data Protection Impact Assessments (Art. 35 GDPR) and in prior consultations with Supervisory Authorities (Art. 36 GDPR), insofar as the Processing under this DPA is concerned.

## 12. Audit Rights

12.1. The Provider shall make available to the Controller all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR. The primary means of verification shall be certificates, audit reports from independent third parties and questionnaires.

12.2. On-site audits are permissible as a last resort if the documentation-based evidence is insufficient. On-site audits are subject to the following conditions:

- at least 30 days' advance notice in text form,
- no more than once per calendar year, unless a concrete occasion requires an additional audit,
- conducted during normal business hours,
- the auditor shall be bound by a confidentiality obligation,
- the costs of the audit shall be borne by the Controller.

## 13. Deletion or Return after Termination

13.1. After termination of the contractual relationship, the Controller shall choose within **30 days** between export/return and deletion of the Personal Data processed on its behalf (Art. 28(3)(g) GDPR).

13.2. Export shall be provided in a machine-readable format appropriate to the respective data type (e.g. JSON/ZIP for metadata, Git archive or TAR for source code, unmodified binaries for artifacts).

13.3. If the Controller does not make a choice within the 30-day period, the Provider shall delete the data from active systems after the period expires.

13.4. **Immutable backups carve-out**: Data in automated, immutable backups shall be deleted during the regular rotation cycle (typically 30–90 days after deletion from active systems). In the meantime, the data shall be isolated, not actively processed and held solely for disaster recovery purposes. This is compatible with Art. 17 GDPR.

13.5. Statutory retention obligations (in particular §§ 147 AO, 257 HGB) shall remain unaffected.

13.6. For the trial period without conversion, a shortened export period of **14 days** (instead of 30 days) shall apply. The remaining provisions of this Section shall apply accordingly.

## 14. Aggregation and Anonymisation

14.1. The Provider may use data arising in the course of the Processing in irreversibly anonymised form for statistical purposes (product improvement, marketing communications).

14.2. Personal end-user data shall not be used by the Provider for its own purposes. In particular, the Provider shall not use customer data for training, fine-tuning or improving AI or ML models.

## 15. Liability

15.1. The liability of the parties shall be governed by the provisions of the Terms of Service. Art. 82 GDPR shall remain unaffected.

## 16. Final Provisions

16.1. The laws of the Federal Republic of Germany shall apply.

16.2. The exclusive place of jurisdiction shall be Konstanz.

16.3. The authoritative language version of this DPA is the English version. The German version is for informational purposes only.

16.4. Should any provision of this DPA be or become invalid, the validity of the remaining provisions shall not be affected. The parties undertake to replace the invalid provision with a valid provision that most closely approximates the economic purpose of the invalid provision.

---

## Annex 1 — Processing Overview

### Purpose of Processing

Provision of the cloud services of the Capawesome Platform commissioned by the Controller.

### Categories of Data Subjects

- End users of the Controller's applications
- Employees and agents of the Controller (insofar as their data is contained in source code, build artifacts or credentials)

### Categories of Personal Data

The following categories describe exclusively data that the Provider processes as Processor on behalf of the Controller.

**Application Delivery Data** Technical identifiers for the delivery of updates and bundles to end-user devices, in particular: app identifier, version information, platform and OS data, installation-specific device identifier, bundle/channel identifier, IP addresses.

**Build Artifacts and Source Code** Source code, compiled artifacts and build logs, insofar as they contain Personal Data (e.g. accidentally hard-coded keys, debug logs with personal test data). Build secrets (Apple API keys, .p12 certificates, provisioning profiles, Android keystores) are primarily customer-confidential security material but regularly contain Personal Data (in particular team name, account e-mail, device UDIDs in provisioning profiles) and accordingly fall within the scope of this DPA including the 48-hour notification obligation under Section 10. The build infrastructure (including Mac build instances for iOS) is provided by the sub-processors listed in Section 7.

**Publishing Artifacts** Store credentials, app binaries and metadata, insofar as they are personal (in the case of Apple provisioning artifacts, practically always).

**Workflow and Integration Data** Webhook payloads and data passed through by configured automations or third-party integrations (e.g. GitHub, GitLab), insofar as they are personal.

### Demarcation — the Provider as Controller

The following data categories are processed by the Provider as an independent Controller and are **not** covered by this DPA:

- Account and organisation metadata
- Authentication data (session/API tokens, SSO attributes)
- Dashboard and CLI telemetry
- Support data

In this regard, the Privacy Policy and the Terms of Service apply.

### Data Export Format

Machine-readable, appropriate to the respective data type (e.g. JSON/ZIP for metadata, Git archive or TAR for source code, unmodified binaries for artifacts). Alternative formats by arrangement.

---

## Annex 2 — Technical and Organisational Measures (TOMs)

The measures below describe the minimum level of security in accordance with Art. 32 GDPR. Changes shall not reduce the level documented in this Annex (see Section 6.2). Supplementary details are documented in the Security Policy at https://capawesome.io/security.

### Confidentiality

- **Access control**: Multi-factor authentication (MFA) for all administrative access to production systems. Principle of least privilege.
- **Customer secrets and credentials**: Apple API keys, .p12 certificates, provisioning profiles and Android keystores are stored encrypted at rest. Access is limited to the automated build/publish pipeline.
- **Customer source code**: Purpose-limited processing in isolated build environments. No access by the Provider's employees outside of a support case with the customer's express authorisation.
- **Employee obligations**: All employees with access to Personal Data are bound by confidentiality obligations.
- **Password policy**: Minimum length and complexity in accordance with the state of the art. Passwords are stored exclusively in hashed form. Use of a password manager.

### Integrity

- **Encryption in transit**: TLS 1.2 or higher for all data transmissions.
- **Encryption at rest**: Industry-standard encryption for stored data.
- **Code signing for live updates**: Bundle signatures are verified client-side before application, ensuring the integrity of delivered updates.
- **Input control**: Logging of which data was entered, modified or deleted, when and by whom.

### Availability and Resilience

- **Redundancy**: Use of redundant server systems and services.
- **Backup and recovery**: Regular, encrypted backups with a documented recovery plan. Regular restore tests.
- **DDoS protection**: Protection measures against denial-of-service attacks.
- **Hosting**: Production systems are operated with carefully selected infrastructure providers (Section 7).

### Regular Review Procedures

- **Certifications**: SOC 2 Type II (auditor and report availability under NDA).
- **Penetration tests**: Annual external penetration tests (from 2026). Reports available under NDA.
- **Monitoring**: Continuous monitoring of systems for security incidents.
- **TOM review**: Regular review and update of the Technical and Organisational Measures.

### Data Separation

- Production and test data are stored strictly separated in different systems.
- Data of different customers is processed in logically separated environments.

---

## Annex 3 — Sub-processors

The current list of Sub-processors is available at https://capawesome.io/subprocessors.

---

## Annex 4 — EU Standard Contractual Clauses

For third-country transfers, the EU Standard Contractual Clauses pursuant to Implementing Decision (EU) 2021/914 of the European Commission of 4 June 2021, Module 3 (Processor to Processor) shall apply.

The SCCs are hereby incorporated by reference into this DPA. The party-specific details (Appendices I–III of the SCCs) are derived from this DPA and its Annexes:

- **Appendix I.A** (Parties): Data exporter (Processor) = Genz IT Solutions GmbH; Data importer (Sub-processor) = as listed in Annex 3
- **Appendix I.B** (Description of processing): As set out in Annex 1 of this DPA
- **Appendix I.C** (Supervisory Authority): Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)
- **Appendix II** (TOMs): As set out in Annex 2 of this DPA
- **Appendix III** (Sub-processors): As set out in Annex 3 of this DPA

Supplementary addenda for transfers under the UK International Data Transfer Addendum (IDTA) and the Swiss revFADP shall be added as further annexes when there is an actual need.