Data Processing Agreement (DPA)

Template version: 1.1
Issued: 16 October 2026
Legal reference: Regulation (EU) 2016/679 (GDPR), Art. 28

> **Disclaimer.** This is DPA template v1.0 pursuant to GDPR Art. 28. Consult your own legal counsel before signing. Cleanthes Apps SRL does not provide legal advice. Placeholders `{{PLACEHOLDER}}` must be filled in at signature.

---

1. Parties

1.1. Controller (Client), hereinafter "Controller":

- Legal name: `{{CLIENT_LEGAL_NAME}}`
- Company registration ID: `{{CLIENT_CUI}}`
- Registered address: `{{CLIENT_ADDRESS}}`
- Legal representative: `{{CLIENT_REPRESENTATIVE}}`, in capacity of `{{CLIENT_REP_TITLE}}`
- Contact email: `{{CLIENT_CONTACT_EMAIL}}`
- Data Protection Officer (DPO), if appointed: `{{CLIENT_DPO}}`

1.2. Processor, hereinafter "Processor":

- Legal name: **Cleanthes Apps SRL**
- Company registration ID: `{{CLEANTHES_CUI}}` *(to be filled once the company is registered)*
- Registered address: `{{CLEANTHES_ADDRESS}}` *(idem)*
- Legal representative: `{{CLEANTHES_REP}}`, in capacity of `{{CLEANTHES_REP_TITLE}}`
- GDPR contact email: `dpo@cleanthes-apps.com`

Jointly referred to as "Parties", individually as "Party".

---

2. Subject matter and purpose

2.1. This Agreement sets out the terms under which the Processor processes personal data on behalf of the Controller, in connection with the software-as-a-service platform **CAP APP** (the "Service").

2.2. This DPA is entered into as a mandatory annex to the Master Service Agreement no. `{{CONTRACT_NUMBER}}` dated `{{CONTRACT_DATE}}` (the "Main Agreement").

2.3. In case of conflict between this DPA and the Main Agreement regarding personal data processing, this DPA prevails.

---

3. Duration

3.1. This Agreement enters into force on `{{EFFECTIVE_DATE}}` and remains valid throughout the term of the Main Agreement.

3.2. The Processor's obligations regarding confidentiality, deletion and return of data survive termination.

---

4. Categories of personal data processed

The Processor processes the following categories of data on behalf of the Controller, via the CAP APP Service:

Category	Concrete examples	Source
Employee identification	Name, employee id, position, department	CSV import / HRIS API from Controller
Professional contact data	Work email, work phone (optional)	Entered by Controller
Professional training data	Skills, courses completed, authorisation start/expiry, evaluation scores	Entered by Controller / trainer
Roles and permissions	Application role (employee/trainer/manager/admin), permissions	Configured by Controller
Technical audit trail	IP address, user agent, action timestamp, action performed	Automatically collected by Service
User-generated content	PDF documents (certificates), profile images (optional), evaluation comments	Entered by Controller / employee

Normally not processed:

- Health data (except medical fitness certificate, if Controller chooses to upload)
- Employee financial/banking data
- Data on political, religious or sexual orientation
- Criminal record data

If the Controller uploads such data, full responsibility for legal basis remains with the Controller.

---

5. Categories of data subjects

- Controller employees with Service accounts (employee, trainer, manager, admin)
- Former Controller employees, until account deletion per retention policy
- Occasional visitors (external auditor, consultant) with temporary accounts granted by Controller

---

6. Processor obligations

The Processor undertakes to:

6.1. **Process data only on the Controller's documented instructions**, including via Service configuration and Main Agreement terms.

6.2. **Ensure confidentiality**: Processor personnel with access to Controller data sign confidentiality undertakings and receive annual GDPR training.

6.3. **Implement appropriate technical and organisational measures** (see section 10).

6.4. **Assist the Controller** in fulfilling its obligations regarding:

- Responses to data subject requests (GDPR Art. 15-22)
- Data protection impact assessment (DPIA)
- Security incident notifications

6.5. **Notify the Controller within 72 hours** of becoming aware of a security incident affecting personal data, by email to `{{CLIENT_CONTACT_EMAIL}}` and to `{{CLIENT_DPO}}` (if appointed).

6.6. **Return or delete all data** upon Main Agreement termination, per section 11.

6.7. **Not transfer data outside the EEA** without safeguards under GDPR Chapter V (SCC, adequacy decisions).

6.8. **Not use the data** for own purposes (marketing, commercial aggregated analytics, external AI model training).

---

7. Controller obligations

7.1. Controller warrants it has valid legal basis for data uploaded to the Service (GDPR Art. 6: typically employment contract execution or legal obligation for authorisations).

7.2. Controller is responsible for configuring roles and permissions in the Service and promptly revoking access for departed personnel.

7.3. Controller informs its employees of processing via the Service, per GDPR Art. 13-14.

7.4. Controller responds to data subject requests received directly. Processor assists technically (export, deletion) within 5 business days.

---

8. Sub-processors

8.1. Controller grants Processor **general authorisation** to engage sub-processors, subject to:

- The list of authorised sub-processors is published in Annex 5 to the Main Agreement and on the website Trust Center page.
- Each sub-processor signs a DPA with Cleanthes Apps SRL with obligations equivalent to those herein.
- Processor notifies Controller at least **30 days** before adding a new sub-processor. Controller may object with reasoned justification; if the objection cannot be resolved, Controller may terminate without penalty.

8.2. **Active sub-processors as of DPA issuance:**

Sub-processor	Role	Processing location	International transfer basis
LowPings Digital Services SRL	Server hosting (application, database, files, backups)	Romania	EU provider, no transfer
Cloudflare Inc.	DNS, CDN and protection (traffic passes encrypted through their network)	EU / global network	SCC + Cloudflare EU DPA
Stripe Payments Europe Ltd	Card payments (subscription and AI credit packages)	Ireland (EU)	EU provider, no transfer

Sub-processor	Role	Processing location	International transfer basis
Anthropic, PBC	AI features: document reading, generated tests, assistant (optional, off by default)	USA	SCC via Anthropic's DPA (only if turned on for Client)

Note: the transactional email provider (notifications, password reset) is chosen in the EU and added to the list with the 30-day notice in art. 8.1. We currently use no third-party error monitoring.

---

9. International data transfer

9.1. Processed data remains in the **European Union** (server: Romania, LowPings).

9.2. Transfers to the US (only the AI features, if turned on, and Cloudflare) rely on:

- Standard Contractual Clauses (SCC) adopted by Decision (EU) 2021/914
- Supplemental technical measures: only what the operation needs is sent, TLS 1.2+ in transit

9.3. Controller receives on request a copy of SCC signed with US sub-processors.

---

10. Technical and organisational security measures

10.1. **Authentication and authorisation:**

- Passwords hashed with bcrypt (cost 12+)
- Two-step sign-in (authenticator app) mandatory for platform administrators; SAML SSO with the company account on the Enterprise plan
- Sessions with expiry, invalidated on sign-out, on password change and with "Sign out of all devices"
- Strict isolation between clients: each request sees only its own client's data, verified by automated tests

10.2. **Encryption:**

- In transit: HTTPS/TLS 1.2+ mandatory, HSTS active
- Passwords and PINs stored only as hashes (bcrypt), never in clear
- Secrets (API keys, DB passwords) stored encrypted, not in Git

10.3. **Audit trail:**

- All critical CRUD actions logged: who, what, when, from what IP
- Log retention: 12 months minimum

10.4. **Backup and recovery:**

- Daily automatic backup (database, files, configuration)
- 90-day retention, on the Service infrastructure in Romania; a copy outside the main server will be added later, with notice to the Controller
- Documented restore procedure; restore test on request
- RTO: 24 hours | RPO: 24 hours

10.5. **Personnel access:**

- Least privilege principle
- Access logs monitored

- Access revoked within 24h of collaboration end

10.6. **Security testing:**

- Dependencies automatically scanned (Dependabot / Renovate)
- Annual pentest planned *(first campaign: Q2 2027, after 5 live clients)*
- Responsible disclosure (policy published on the website)

---

11. Data retention and deletion

11.1. **During contract:** Processor retains data per Controller configuration.

11.2. **Standard retention policy:**

- Audit logs (action logs): 12 months rolling
- Backups: 90 days
- Account deactivated by Controller: 30 days grace, then anonymisation

11.3. **Upon contract termination:**

- Controller can export its data (CSV / PDF / JSON) for 30 days
- After those 30 days, data is permanently deleted from production, with an email warning beforehand
- Backups expire naturally within 90 days
- Deletion certificate provided on request

11.4. Controller may request early deletion via written request to `dpo@cleanthes-apps.com`.

---

12. Data subject rights

12.1. Data subject requests are addressed primarily to Controller. Processor assists technically:

- Personal data export (Art. 15 access / Art. 20 portability): delivered in 5 business days
- Rectification of incorrect data, reflected immediately (Controller modifies via UI)
- Data deletion (Art. 17): reflected within 30 days
- Restriction / objection: Processor suspends account access at Controller request

12.2. If a data subject contacts Processor directly, Processor redirects the request to Controller and informs the subject within 5 business days.

---

13. Audit rights

13.1. Controller may verify Processor compliance:

- Via annual security questionnaire (Processor responds in 30 days)
- Via document request (Security Whitepaper, compliance matrix, pentest report when available)
- Via on-site audit with 60-day notice, in business hours, Controller bearing costs (if audit identifies no material non-compliance)

13.2. Processor may substitute third-party audit reports (e.g. ISO 27001): *this certification is in preparation, planned for 2027. Until then: Security Whitepaper + compliance matrix + questionnaire response.*

---

14. Review

14.1. This DPA is reviewed annually or on changes to applicable law.

14.2. Changes unfavorable to Controller are notified at least 90 days in advance. Controller may terminate without penalty during this period.

---

15. Governing law and jurisdiction

15.1. This DPA is governed by the laws of Romania and by GDPR.

15.2. Disputes are settled amicably; failing that, by the courts of **Timisoara, Romania**.

15.3. Data subjects may lodge complaints with **ANSPDCP** (Romanian Data Protection Authority), https://www.dataprotection.ro.

---

16. Signatures

Controller:

Full name: `{{CLIENT_REPRESENTATIVE}}`
Title: `{{CLIENT_REP_TITLE}}`
Date: `{{SIGNATURE_DATE}}`

Signature + stamp: `{{CLIENT_SIGNATURE}}`

Processor: Cleanthes Apps SRL

Full name: `{{CLEANTHES_REP}}`
Title: `{{CLEANTHES_REP_TITLE}}`
Date: `{{SIGNATURE_DATE}}`

Signature + stamp: `{{CLEANTHES_SIGNATURE}}`

Issued in two original copies, one for each Party.
DPA Template v1.0, 28 August 2026, Cleanthes Apps SRL