CLEVERA TEKNOLOJI A.Ş.

Data Processing Addendum

Version 1.0 **Effective date** 14 November 2026 **Published at** clevera.ai/dpa

---

This Data Processing Addendum ("**DPA**") is entered into between:

1. **Clevera Teknoloji Anonim Şirketi** ("Clevera Teknoloji A.Ş."), a joint stock company incorporated in the Republic of Türkiye, registered with the Sivas Trade Registry (Sivas Ticaret Sicili Müdürlüğü) under no. 23130, MERSİS no. 0211156884000001, tax office Site, tax no. 2111568840, with its registered address at Yenişehir Mah. Kardeşler Cad. Tekno Kent Arge No: 7/2 İç Kapı No: B14, Merkez / Sivas, Türkiye ("**Clevera**"); and
2. **the customer** that has agreed to the Clevera Terms of Service or another written agreement with Clevera for the Service, as identified in its Clevera account, in an order form or in the signature block of a signed copy of this DPA ("**Customer**").

Clevera and the Customer are each a "**party**" and together the "**parties**".

How this DPA applies

(a) Part of the Agreement. This DPA forms part of the Clevera Terms of Service at https://www.clevera.ai/terms, or of any other written agreement between the parties for the Service (the "**Agreement**"). It applies automatically, without signature, to every Customer whenever Clevera Processes Customer Personal Data on the Customer's behalf, from the later of the effective date above and the date on which the Customer accepted the Agreement.

(b) Signed copies. A Customer that wants a signed copy may download the copy of this DPA signed by Clevera from https://www.clevera.ai/dpa, countersign it and send it to privacy@clevera.ai. Countersigning does not change the terms of this DPA, and this DPA applies whether or not the Customer countersigns it.

(c) No negotiation, except Custom plans. Clevera does not agree changes to this DPA, except for Customers on a Custom plan, and then only in a separate written agreement signed by both parties.

(d) Language. This DPA is written in English. Any translation is provided for convenience only. If a translation conflicts with the English version, the English version prevails.

1. Definitions

Terms that are not defined in this DPA have the meaning given in the Agreement or in Data Protection Law.

- **"Authorized Users"** means the people the Customer allows to use the Service under its account, such as members of its workspaces, whatever their role.
- **"Controller"**, **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Processing"** (and **"Process"**), **"Personal Data Breach"** and **"Supervisory Authority"** have the meanings given in the GDPR. Under other Data Protection Law they mean the equivalent terms, such as "business", "service provider" and "personal information" under the CCPA, and "data controller" and "data processor" under the KVKK.

- **"Customer Content"** has the meaning given to "Your Content" in the Terms of Service: everything the Customer or its Authorized Users put into the Service (recordings, uploads, links, scripts, instructions, website captures and data) and the output the Service generates for the Customer (videos, social clips, narration, captions, articles, images and translations). It includes the content of the Customer's Help Centers.
- **"Customer Personal Data"** means Personal Data in Customer Content, and Personal Data of Help Center Readers, that Clevera Processes on the Customer's behalf under the Agreement. It does not include the data described in section 2.4.
- **"Data Protection Law"** means all laws that apply to the Processing of Customer Personal Data under the Agreement, including, where applicable: Regulation (EU) 2016/679 (the "**GDPR**"); the GDPR as it forms part of the law of the United Kingdom and the UK Data Protection Act 2018 (together, the "**UK GDPR**"); the Swiss Federal Act on Data Protection of 25 September 2020 (the "**FADP**"); the Turkish Law on the Protection of Personal Data No. 6698 (the "**KVKK**"); and the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (the "**CCPA**"), in each case together with its implementing regulations.
- **"Help Center"** means a documentation site or help center that the Customer creates and publishes with the Service, on a Clevera domain (such as a subdomain of clevera.help) or on the Customer's own domain.
- **"Help Center Readers"** means visitors to a Customer's Help Center, including people who use its search, its Ask AI assistant, its feedback buttons or its contact form.
- **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **"Service"** means the Clevera services provided under the Agreement, including the web app at app.clevera.ai, the desktop recorder, the Chrome extension, the APIs and MCP server, shared video pages and embeds, and Help Centers. It does not include the free tools at clevera.ai/tools, which are used without an account and for which Clevera is the Controller.
- **"Sub-processor"** means any third party engaged by Clevera that Processes Customer Personal Data on Clevera's behalf.
- **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, version B1.0, in force from 21 March 2022, as amended from time to time.

2. Scope and roles

2.1 Roles. For Customer Personal Data, the Customer is the Controller, or a Processor acting on behalf of its own Controller, and Clevera is the Customer's Processor, or Sub-processor. Where the Customer acts as a Processor, the Customer warrants that its Controller has authorised the Customer's instructions and the engagement of Clevera, including the engagement of Sub-processors under section 6. The Customer remains Clevera's only point of contact and is responsible for passing on any notice or information to its Controller.

2.2 Subject matter, nature and purpose. Clevera Processes Customer Personal Data only to provide the Service to the Customer, as described in Annex I. This consists of storing, analysing and transforming Customer Content, with AI models and other tools, to produce videos, social clips, narration, captions, articles, translations and Help Centers; hosting and delivering that content; and the related support, security and abuse prevention.

2.3 Duration. This DPA applies for as long as Clevera Processes Customer Personal Data, including after the Agreement ends, until that data is deleted under section 11.

2.4 Data for which Clevera is a Controller. As Clevera's Privacy Policy at https://www.clevera.ai/privacy describes, Clevera is a Controller, not a Processor, for: account data of Authorized Users; billing and usage data; security and login data; data from its own website, including the free tools; marketing; and support conversations. This DPA does not apply to that data, which Clevera Processes under its Privacy Policy and Data Protection Law.

2.5 Payments. Payments for the Service are processed by Lemon Squeezy, which acts as Merchant of Record and as an independent Controller under its own terms and privacy policy. Lemon Squeezy is not a Sub-processor under this DPA.

3. Instructions and Customer responsibilities

3.1 Instructions. Clevera Processes Customer Personal Data only on the Customer's documented instructions, including with regard to transfers to a third country, unless Union or Member State law, or other law to which Clevera is subject, requires otherwise. In that case Clevera will inform the Customer of that legal requirement before Processing, unless that law prohibits this on important grounds of public interest. The Customer's complete documented instructions at the effective date are: (a) the Agreement and this DPA; (b) the Customer's and its Authorized Users' use and configuration of the Service, such as starting a job, connecting an integration, publishing a Help Center or turning on "Remember my sign-in"; and (c) any other written instructions that the parties agree.

3.2 Unlawful instructions. Clevera will inform the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Law. Clevera may suspend the Processing concerned until the Customer confirms, withdraws or changes the instruction.

3.3 Customer responsibilities. The Customer is responsible for:

- (a) having a lawful basis for the Customer Personal Data it puts into the Service and for its instructions, and for giving any notices and obtaining any consents that Data Protection Law requires, including from people who appear or are heard in recordings and people whose data appears on screen;
- (b) pointing the Service only at websites and accounts that it owns or is authorised to use in this way, and using test or demo accounts where possible;
- (c) not submitting highly sensitive data, including health data subject to HIPAA, payment card data and government identification numbers, and not submitting special categories of personal data (GDPR Article 9) or personal data relating to criminal convictions and offences (GDPR Article 10), unless Clevera has agreed to this in advance in writing;
- (d) the privacy notices, cookie notices and lawful basis for its Help Centers, including any third-party analytics or other services it adds to a Help Center itself (such as Google Analytics, Plausible, PostHog or Segment), which act for the Customer and are not Clevera's Sub-processors;
- (e) the security of its accounts, including its Authorized Users' credentials, two-factor authentication and, where available, its single sign-on configuration; and
- (f) reviewing AI-generated output before publishing or relying on it.

3.4 Services the Customer connects. Third-party services that the Customer connects to the Service, or to which the Customer directs Clevera to send data, act on the Customer's instructions and under their own terms. They are not Clevera's Sub-processors. They include: ElevenLabs used with the Customer's own API key; publishing and import integrations such as Notion, Confluence, GitHub, GitLab, Bitbucket, ClickUp, Google Docs, Help Scout, GitBook, ReadMe and WordPress; the video, social and storage platforms listed in the Privacy Policy; the Customer's own identity provider used for single sign-on; and the Clevera app for Slack, when the Customer installs it in its own Slack workspace.

4. Confidentiality

Clevera ensures that every person it authorises to Process Customer Personal Data, including its employees and contractors, is bound by an appropriate obligation of confidentiality, whether contractual or statutory. Clevera limits access to Customer Personal Data to those persons who need it to provide the Service. Clevera staff look at Customer Content only to provide support that the Customer requests, to investigate abuse or a security incident, or where the law requires it.

5. Security

5.1 Measures. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing, as well as the risks to Data Subjects, Clevera implements and maintains the technical and organisational measures described in Annex II, which are designed to ensure a level of security appropriate to the risk, as required by GDPR Article 32.

5.2 Updates. Clevera may update the measures in Annex II as technology and threats develop, provided that an update does not materially reduce the overall level of security of the Service.

6. Sub-processors

6.1 General authorisation. The Customer gives Clevera a general written authorisation to engage Sub-processors. The Sub-processors listed in Annex III are authorised as of the effective date of this DPA. Clevera keeps the current list at https://www.clevera.ai/subprocessors.

6.2 Sub-processor obligations. Clevera engages each Sub-processor under a written contract that imposes on the Sub-processor data protection obligations that are, in substance, no less protective than those in this DPA, to the extent they apply to the service the Sub-processor provides. Clevera remains fully liable to the Customer for the performance of each Sub-processor's obligations.

6.3 Notice of changes. Clevera will give notice of any intended addition or replacement of a Sub-processor at least 30 days before the new Sub-processor starts Processing Customer Personal Data. Clevera gives notice by updating https://www.clevera.ai/subprocessors and by email to the owners of the Customer's workspaces.

6.4 Right to object. The Customer may object to a new Sub-processor on reasonable grounds relating to data protection by writing to privacy@clevera.ai before the end of the notice period. The parties will discuss the objection in good faith. Clevera may propose a reasonable alternative, such as a change to the Customer's configuration or use of the Service that avoids the new Sub-processor. If the objection is not resolved within the notice period, the Customer may terminate the affected part of the Service, or the Agreement, by written notice to Clevera with effect from the date the new Sub-processor would start Processing Customer Personal Data, and Clevera will refund the prepaid fees for the period after termination on a pro-rata basis. This refund is a written statement for the purposes of the refund section of the Terms of Service.

7. International transfers

7.1 Locations. Clevera is established in Türkiye. Customer Personal Data is processed mainly in the European Union and the United States. Clevera's application servers and database run at Hetzner in Germany. Recordings, uploads and generated media are stored at Amazon Web Services in the United States, and public brand assets in the European Union (Sweden). Media and Help Centers are delivered

through Amazon CloudFront, which serves content from locations worldwide. Server renders run on AWS Lambda in the United States. Most AI and other Sub-processors process data in the United States, as shown in Annex III. Clevera does not currently offer customer-selectable data residency.

7.2 Transfers subject to the GDPR. To the extent that the Customer's transfer of Customer Personal Data to Clevera, or Clevera's Processing, is a transfer of personal data to a third country that is subject to the GDPR and is not covered by an adequacy decision, the SCCs are incorporated into this DPA by reference and apply as follows:

- (a) **Module Two** (controller to processor) applies where the Customer is a Controller, and **Module Three** (processor to processor) applies where the Customer is a Processor;
- (b) the Customer is the data exporter and Clevera is the data importer;
- (c) Clause 7 (docking clause) is included;
- (d) in Clause 9(a), **Option 2** (general written authorisation) applies, and the time period for prior notice of changes is 30 days, as set out in section 6.3;
- (e) in Clause 11(a), the optional language does not apply;
- (f) in Clause 13, the competent Supervisory Authority is determined in accordance with Clause 13(a) and Annex I.C;
- (g) in Clause 17, **Option 1** applies, and the SCCs are governed by the law of Ireland;
- (h) in Clause 18(b), disputes are resolved before the courts of Ireland;
- (i) Annexes I, II and III of the SCCs are completed with the information in Annexes I, II and III of this DPA.

7.3 Onward transfers. Where a Sub-processor Processes Customer Personal Data in a country outside the EEA that is not covered by an adequacy decision, Clevera ensures that the onward transfer complies with Clause 8.7 (Module Two) or Clause 8.8 (Module Three) of the SCCs, by relying on the Sub-processor's certification under the EU–U.S. Data Privacy Framework where the Sub-processor is certified, or on standard contractual clauses between Clevera and the Sub-processor.

7.4 Transfers subject to the UK GDPR. For transfers subject to the UK GDPR, the UK Addendum is incorporated into this DPA by reference and applies as follows: Table 1 is completed with the parties' details in Annex I; Table 2 is completed with the selections in section 7.2; Table 3 is completed with Annexes I, II and III of this DPA; and in Table 4, neither party may end the UK Addendum when the Approved Addendum changes.

7.5 Transfers subject to the FADP. For transfers subject to the FADP, the SCCs apply as set out in section 7.2, with these changes: references to the GDPR are read as references to the FADP to the extent the transfer is subject to it; the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner; the term "Member State" in Clause 18(c) does not exclude Data Subjects in Switzerland from bringing claims in Switzerland, where they have their habitual residence, in accordance with Clause 18(c).

7.6 Transfers subject to the KVKK. Where the KVKK applies to a transfer of Customer Personal Data outside Türkiye, including an onward transfer to a Sub-processor, the transfer is made in accordance with Article 9 of the KVKK. Where no adequacy decision applies, the parties rely on the standard contracts announced by the Turkish Personal Data Protection Board, completed with the information in Annexes I to III of this DPA, and the party that the KVKK requires to do so notifies the Turkish Personal Data Protection Authority of the standard contract within five business days of its signature.

7.7 Alternative transfer mechanisms. If a transfer mechanism relied on in this section 7 is invalidated, amended or replaced, the parties will cooperate in good faith to put in place a lawful alternative, and Clevera may adopt a successor mechanism by notice under section 15.

8. Assistance to the Customer

8.1 Data Subject requests. Taking into account the nature of the Processing, Clevera assists the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects to exercise their rights. The Customer can meet most requests through the Service, which lets it view, edit, export and delete Customer Content. If Clevera receives a request directly from a Data Subject about Customer Personal Data, Clevera will not respond to it, except to refer the Data Subject to the Customer, unless the Customer instructs otherwise or the law requires it. Where Clevera can identify the Customer concerned, it will inform the Customer of the request without undue delay.

8.2 Impact assessments and consultation. Taking into account the nature of the Processing and the information available to it, Clevera provides reasonable assistance to the Customer with data protection impact assessments and prior consultations with Supervisory Authorities that relate to the Customer's use of the Service, mainly by providing this DPA, the Security page at https://www.clevera.ai/security and the information described in section 10.

8.3 Cost of assistance. Assistance through the self-service features of the Service and Clevera's standard documentation is free. For assistance that goes beyond this, Clevera may charge its reasonable costs, which it will agree with the Customer in advance.

9. Personal Data Breaches

9.1 Notification. Clevera will notify the Customer of a Personal Data Breach affecting Customer Personal Data without undue delay, and in any event within 72 hours, after becoming aware of it.

9.2 Content. The notification will describe, to the extent the information is then available: the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and of personal data records concerned; the likely consequences of the Personal Data Breach; the measures taken or proposed to address it, including measures to mitigate its possible adverse effects; and a contact point where more information can be obtained. Where Clevera cannot provide all of this information at the same time, it will provide it in phases without undue further delay.

9.3 Channel. Clevera sends the notification by email to the owners of the Customer's affected workspaces. The Customer is responsible for keeping those email addresses current. The Customer can report a suspected security incident affecting the Service to security@clevera.ai.

9.4 Response and cooperation. Clevera will take reasonable steps to contain, investigate and remedy the Personal Data Breach and will cooperate with the Customer so that the Customer can meet its own obligations to notify Supervisory Authorities and Data Subjects.

9.5 No admission. Clevera's notification of, or response to, a Personal Data Breach is not an acknowledgement of fault or liability.

10. Information and audits

10.1 Information. Clevera makes available to the Customer, on written request to privacy@clevera.ai, the information reasonably necessary to demonstrate compliance with the obligations in GDPR Article 28 and this DPA. This includes this DPA, the Security page, the current Sub-processor list, Clevera's answers to a reasonable security questionnaire and, once available, third-party audit reports.

10.2 Certifications. As stated on Clevera's Security page, Clevera's SOC 2 audit is in progress, expected in 2027, and Clevera plans to obtain ISO 27001 certification in 2027. Clevera does not currently hold either certification. Once a SOC 2 report has been issued, Clevera will make it available on request under appropriate confidentiality terms.

10.3 Reports and questionnaires first. The Customer agrees to exercise its audit rights first by reviewing the information described in section 10.1. The Customer may send a written security questionnaire at most once in any 12-month period, except after a Personal Data Breach, where a Supervisory Authority requires it, or where there are indications of non-compliance with this DPA. Clevera will answer within a reasonable time.

10.4 Audits and inspections. If the information provided under sections 10.1 to 10.3 is not sufficient to demonstrate Clevera's compliance with this DPA, or if a Supervisory Authority requires it, the Customer may carry out an audit, including an on-site inspection, itself or through an independent auditor that is bound by confidentiality obligations and is not a competitor of Clevera. The Customer must give at least 30 days' written notice and agree the scope, timing and duration of the audit with Clevera in advance. The audit will take place during normal business hours, no more than once in any 12-month period (except after a Personal Data Breach, where a Supervisory Authority requires it, or where there are indications of non-compliance), and in a way that minimises disruption to Clevera's business. The audit does not extend to the data of Clevera's other customers or to Sub-processors' facilities, for which Clevera will make available the Sub-processors' own audit reports or certifications where it can. The Customer bears its own costs of any audit and reimburses Clevera's reasonable costs of an on-site inspection, except where the inspection shows that Clevera has materially breached this DPA. The Customer will give Clevera a copy of any audit report free of charge.

10.5 Supervisory Authorities. Nothing in this section 10 limits the rights of a Supervisory Authority or of Data Subjects under the SCCs or Data Protection Law.

11. Return and deletion

11.1 During the term. The Customer can delete Customer Content at any time using the Service. Items moved to trash are permanently deleted after 7 days, and recordings that are not used in any video are deleted 15 days after their last use.

11.2 Export. Before deleting a workspace or account, the Customer can export Customer Content with the export features of the Service, for example videos as files on paid plans and Help Centers as HTML or Markdown. Deleted Customer Content cannot be restored, so the Customer must export anything it wants to keep before deletion.

11.3 Deletion when a workspace or account is deleted. When the Customer deletes a workspace, or the owner of a workspace deletes their account, deletion starts at once. Access to the workspace ends, its subscription is cancelled, its integrations, access tokens and saved browser sign-ins are revoked or deleted, including the saved browser profiles held by Browser Use, and its Help Centers stop being served. Clevera then permanently deletes the remaining Customer Content of the workspace, including its recordings, videos and files and the corresponding stored objects at Amazon Web Services, its Help Centers and their hosted files, and its Help Center Reader data. This is done by an automated process that runs continuously and completes without undue delay, and in any event within 30 days. Items in trash are deleted in the same process and are not kept for the remainder of the trash period. Copies of deleted data in Clevera's database backups are deleted automatically when those backups expire, within 7 days after the data is deleted from the live systems.

11.4 Help Center Reader data. Unless the Customer deletes it sooner or deletes the Help Center, Clevera keeps Help Center Reader data as follows: Ask AI conversations, search events, page views and feedback for 13 months; contact-form messages for 180 days; cached answers to repeated Ask AI questions for 7 days;

and the raw request logs from which page views and searches are counted for 30 days.

11.5 Retention required by law. Clevera may keep Customer Personal Data where Union or Member State law, or other law to which Clevera is subject, requires it to do so, and then only for as long as that law requires. Clevera will keep that data confidential and Process it only for the purpose for which the law requires it to be kept.

11.6 Confirmation. On written request, Clevera will confirm in writing that deletion under this section 11 has been carried out.

12. CCPA and other US state privacy laws

12.1 Roles. Where the CCPA or a similar US state privacy law applies, the Customer is a "business" and Clevera is a "service provider" (or "processor") for Customer Personal Data. Clevera Processes Customer Personal Data only for the limited and specified business purposes of providing the Service, as described in the Agreement and Annex I.

12.2 Restrictions. Clevera will not: (a) sell or share Customer Personal Data, as "sell" and "share" are defined in the CCPA, including for cross-context behavioral advertising; (b) retain, use or disclose Customer Personal Data for any purpose other than the business purposes in section 12.1, or outside the direct business relationship between Clevera and the Customer, except as the CCPA permits; or (c) combine Customer Personal Data with personal information that Clevera receives from or on behalf of another person, or collects from its own interactions with a consumer, except as the CCPA permits.

12.3 Compliance. Clevera will comply with the obligations that apply to it under the CCPA and provide the same level of privacy protection that the CCPA requires of businesses. Clevera will notify the Customer if it determines that it can no longer meet its obligations under the CCPA. The Customer may then take reasonable and appropriate steps to stop and remediate any unauthorised use of Customer Personal Data.

12.4 Oversight. The Customer may take reasonable and appropriate steps to ensure that Clevera uses Customer Personal Data in a manner consistent with the Customer's obligations under the CCPA, through the information and audit rights in section 10.

12.5 Certification. Clevera certifies that it understands the restrictions in this section 12 and will comply with them.

13. Liability

Each party's liability arising out of or in connection with this DPA, and the SCCs where they apply, whether in contract, tort or under any other theory of liability, is subject to the limitations and exclusions of liability in the Agreement, including the limit of the amounts the Customer paid or owed in the 12 months before the event giving rise to the claim. This section does not limit either party's liability to Data Subjects under the SCCs or under Data Protection Law where that law does not allow it to be limited.

14. Order of precedence

If there is a conflict between the documents that make up the agreement between the parties, the following order applies: (1) the SCCs and the UK Addendum, where they apply; (2) this DPA; (3) the rest of the Agreement. Otherwise, the Agreement remains unchanged and in full force.

15. Changes to this DPA

15.1 Updates. Clevera may update this DPA only: (a) where a change in Data Protection Law, a decision of a court or Supervisory Authority, or official guidance requires it; (b) to adopt new or successor transfer mechanisms, such as new standard contractual clauses; or (c) in a way that does not materially reduce the protection given to Customer Personal Data. Clevera will publish each version at https://www.clevera.ai/dpa with its version number and effective date, and will give at least 30 days' notice of a material update by email to the owners of the Customer's workspaces, unless a shorter period is required to comply with law. Changes to Sub-processors follow section 6.

15.2 Signed copies. An update made under section 15.1 also applies to a Customer that has countersigned an earlier version of this DPA. A change that materially reduces the protection given to Customer Personal Data requires the Customer's written agreement.

16. Governing law and jurisdiction

Except where the SCCs, the UK Addendum or Data Protection Law require otherwise, this DPA is governed by the laws of the Republic of Türkiye, excluding its conflict-of-law rules, and the courts of Sivas, Türkiye have exclusive jurisdiction over any dispute arising out of or in connection with it, consistent with the Terms of Service. The SCCs are governed by the law of Ireland, and disputes under them are resolved before the courts of Ireland, as set out in section 7.2.

17. Term

This DPA remains in effect for as long as Clevera Processes Customer Personal Data and ends automatically when Clevera no longer does so. Provisions that by their nature should survive the end of this DPA will survive.

18. Contacts

- Privacy, this DPA, objections to Sub-processors and requests under sections 8, 10 and 11: privacy@clevera.ai
- Security incidents: security@clevera.ai

Signatures

Clevera Teknoloji A.Ş.

Signature	*/s/ Berkay Akpolat*
Name	Berkay Akpolat
Title	Chairman of the Board (Yönetim Kurulu Başkanı)
Date	14 November 2026

Customer

Company	
Name	
Title	
Date	
Signature	

Countersigning is optional: this DPA applies to every Customer as part of the Agreement. To keep a signed copy, complete the Customer block and email this document to privacy@clevera.ai.

Annex I — Description of the Processing

A. List of parties

Data exporter

- Name: the Customer, as identified in its Clevera account, an order form or the signature block above.
- Address and contact person: as set out in the Customer's Clevera account or the signature block above.
- Activities relevant to the transfer: use of the Service.
- Role: Controller (Module Two) or Processor (Module Three).
- Signature and date: by accepting the Agreement, or as set out in the signature block above.

Data importer

- Name: Clevera Teknoloji Anonim Şirketi (Clevera Teknoloji A.Ş.).
- Address: Yenişehir Mah. Kardeşler Cad. Tekno Kent Arge No: 7/2 İç Kapı No: B14, Merkez / Sivas, Türkiye.
- Contact person: Berkay Akpolat, Chairman of the Board, privacy@clevera.ai.
- Clevera has not appointed a data protection officer or a representative in the European Union or the United Kingdom.
- Activities relevant to the transfer: provision of the Service.
- Role: Processor.
- Signature and date: as set out in the signature block above.

B. Description of the transfer

Categories of Data Subjects

- Authorized Users, to the extent their data appears in Customer Content (for example their voice, face or name in a recording).
- People who appear, are heard or are named in Customer Content, such as the Customer's employees, customers, end users and partners and other people visible in screen recordings, camera video, uploaded materials, website captures or the Customer's software.
- People whose details appear on websites or in accounts that the Customer directs Clevera to research or film.
- People whose details appear in content the Customer imports from other tools, such as help-center articles imported from third-party platforms.
- Help Center Readers, including people who contact the Customer through a Help Center's contact form.

Categories of personal data

- Recordings: screen video and, where turned on, camera video and microphone audio; and, from the desktop recorder, interaction data such as clicks, scrolls, key presses, cursor movement and, where the recorder captures it, text typed during the recording. The Chrome extension records video and sound only.
- Any personal data visible or audible in recordings, uploaded materials (images, videos, audio and PDFs) and website captures, such as names, email addresses, profile photos, account details and other data displayed by the Customer's software.

- Voice: recorded voice and voice-over narration generated from text.
- Generated output that contains personal data: scripts, narration, captions, transcripts, AI avatar videos, articles and translations.
- Instructions given to in-app assistants.
- Credentials that the Customer provides for a "Record with AI" run, which are held encrypted only while the run lasts, and saved browser sign-in cookies where the Customer turns on "Remember my sign-in".
- Help Center content published by the Customer.
- Help Center Reader data: Ask AI questions and answers, linked to a hashed visitor identifier; search queries; page views and feedback (including optional comments), with country, device type, language and referring site; contact-form submissions (name, email address, message, page, language, country and a hashed IP address); request logs, which contain IP addresses; and the data needed to control access to restricted Help Centers.
- Shared-video viewer data: device class and country.

Sensitive data transferred

None is intended. Under section 3.3(c), the Customer must not submit special categories of personal data or data relating to criminal convictions and offences without Clevera's prior written agreement. Such data may nonetheless appear incidentally in recordings or materials. The safeguards that apply are the measures in Annex II, in particular encryption in transit, access controls, signed links that expire, and limited retention.

Frequency of the transfer: continuous, for the duration of the Agreement.

Nature of the Processing: collection by upload or capture; storage; analysis with AI models, including transcription, vision analysis, script writing, translation, text-to-speech, embeddings and avatar generation; rendering; hosting and delivery, including Help Center hosting and Ask AI answers based on the Customer's published Help Center content; retrieval; and deletion.

Purpose of the Processing and of the transfer: to provide the Service to the Customer under the Agreement, including support the Customer requests, security and abuse prevention.

Retention period: as set out in section 11.

Transfers to Sub-processors: to the Sub-processors listed in Annex III, for the purposes, data and locations set out there, for the duration of the Agreement.

C. Competent Supervisory Authority

The Supervisory Authority determined in accordance with Clause 13(a) of the SCCs: where the Customer is established in an EU Member State, the Supervisory Authority of that Member State; where the Customer is not established in the EU but falls within Article 3(2) of the GDPR and has appointed a representative under Article 27(1) of the GDPR, the Supervisory Authority of the Member State in which that representative is established; and where the Customer is not established in the EU, falls within Article 3(2) of the GDPR and has not appointed a representative, the Supervisory Authority of the Member State in which the Data Subjects whose personal data is transferred are located. For transfers subject to the UK GDPR, the UK Information Commissioner; for transfers subject to the FADP, the Swiss Federal Data Protection and Information Commissioner.

Annex II — Technical and organisational measures

1. Encryption

- TLS for all traffic to the Service.
- Application-level encryption at rest of integration OAuth tokens, single sign-on secrets, the Customer's own provider API keys, temporary website credentials and provider download links.
- Passwords stored only as one-way hashes.
- Stored files encrypted at rest by the storage provider (Amazon S3 server-side encryption).
- Database backups stored in cloud object storage, encrypted at rest by the storage provider.

2. Access control in the product

- Two-factor authentication with authenticator-app (TOTP) codes and recovery codes.
- New-device verification: a one-time code sent by email when a user signs in from a new device or location, with periodic re-verification of trusted devices.
- Check of new passwords against known breached passwords at registration and password change, using a k-anonymity range query that sends only the first five characters of the password's hash.
- Single sign-on with SAML 2.0 and OpenID Connect on Custom plans, with optional enforcement.
- Team roles (Owner, Administrator, Editor and Content Creator) that control what each member can see and change.
- Rate limiting of sign-in, two-factor, verification and API endpoints.
- Desktop recorder API tokens that are scoped to recording and can be revoked.

3. Internal access control

- Access to production systems limited to authorised staff who need it.
- Administrative tools in the app protected by a separate admin role.
- Staff access to Customer Content only to provide support the Customer requests, to investigate abuse or a security incident, or where the law requires it.
- Least-privilege service credentials, with secrets kept outside source control.

4. Infrastructure and network

- Application servers at Hetzner in Germany, managed with Laravel Forge. The database and queue accept connections only from the application servers, not from the internet.
- Private media served only through signed links that expire, typically within 24 hours. Uploads go directly to storage through single-use pre-signed URLs.
- Isolation of the components that visit websites: Clevera's own site scanner runs as a separate, restricted system user with no access to API keys, behind an outbound firewall that blocks internal networks and cloud metadata endpoints. AI-driven browsing runs in isolated cloud browsers at Browser Use, outside Clevera's infrastructure.

5. Credentials for "Record with AI"

- Credentials passed to the browser as secrets, never placed in the AI model's prompt, and redacted from logs.
- Credentials held encrypted on Clevera's side only while the run lasts, and then discarded.

- Saved sign-ins off by default and enabled per site; removable at any time; deleted after 30 days without use, and when the account or workspace is deleted.
- Confirmation by the person setting up a run that they are allowed to give Clevera access to the account.

6. Application security

- Code review and automated tests for every change.
- Framework protections, including CSRF tokens, output escaping, parameterised database queries and signed cookies.
- Sanitisation of uploaded SVG files.
- Content-Security-Policy restrictions on which sites can be embedded in the app.
- Signature verification of incoming webhooks.
- Penetration tests of the Service.

7. AI providers and data minimisation

- AI providers used under commercial API terms that do not allow them to train their models on Customer Content. Clevera does not use Customer Content to train AI models.
- Each AI provider receives only the data the job needs.
- Video files uploaded to an AI provider for analysis are deleted from the provider within hours of the job. Some providers keep API inputs and outputs for a limited period, typically up to 30 days, for abuse monitoring.
- Keyed hashes instead of raw IP addresses for abuse prevention and Help Center analytics; only device class and country for shared-video analytics.

8. Organisational measures

- Security and data protection training for staff.
- Confidentiality agreements with all staff.
- Background checks on staff.
- Device security rules for the computers and phones staff use for work.

9. Logging, monitoring and incident response

- Application and security logs kept for about 14 to 30 days.
- Alerts on elevated error rates, failed jobs and unusual usage.
- A defined process to triage, contain and fix security incidents and to notify Customers under section 9.
- A vulnerability disclosure process through security@clevera.ai, with a good-faith safe harbour.

10. Availability and resilience

- Daily database backups, kept for 7 days and then deleted automatically.
- Services that can be redeployed from source control.
- Long-running jobs queued and retried on failure.

11. Retention and deletion

- Automatic deletion of trashed items after 7 days and of unused recordings after 15 days.
- Automated deletion of workspaces and accounts, as described in section 11.
- Automatic deletion of Help Center Reader data after the periods in section 11.4.

12. Assistance to the Customer

- Self-service viewing, editing, export and deletion of Customer Content, and role-based access, as described in section 8.

13. Sub-processors

- Written contracts with data protection obligations under section 6.2, and transfer safeguards under section 7.3.

Annex III — Sub-processors

The current list of Sub-processors is published at https://www.clevera.ai/subprocessors. Changes are announced as set out in section 6.3. As of the effective date of this DPA, Clevera uses the following Sub-processors:

Sub-processor	Purpose	Customer Personal Data	Location
Amazon Web Services, Inc.	Storage of recordings, uploads and generated media (Amazon S3); media delivery (Amazon CloudFront); server rendering (AWS Lambda); Help Center hosting and delivery (Amazon S3, Amazon CloudFront, AWS Lambda and Amazon SQS); service email delivery (Amazon SES)	Customer Content; Help Center content and Help Center Reader data; email addresses and the content of service emails	United States; EU (Sweden) for public brand assets and email; CloudFront locations worldwide for delivery
Hetzner Online GmbH	Application servers and database	All Customer Personal Data held in the application database	EU (Germany)
Laravel Holdings Inc. (Laravel Forge)	Provisioning and management of the application servers, and daily database backups	Customer Personal Data on the servers it manages and in database backups	United States
Laravel Holdings Inc. (Laravel Nightwatch)	Application monitoring and error tracking	Technical logs that may include user identifiers and request details	United States
Google LLC (Gemini API, Cloud Text-to-Speech)	AI analysis of recordings, websites and materials; script writing, translation and narration; image generation; Help Center Ask AI answers and question suggestions	Customer Content; Help Center content; Ask AI questions	United States
Anthropic, PBC	AI models that write and direct videos and social clips, and the in-app assistant	Customer Content; assistant instructions	United States
OpenAI, L.L.C.	Speech-to-text transcription and captions; AI models, including the model that drives website research; text embeddings for Help Center search and Ask AI	Recorded audio, narration and Customer Content; website pages; Help Center content; Ask AI questions	United States
Browser Use	Cloud browsers for AI website research and "Record with AI"	Website addresses and pages visited; credentials provided for a run; saved sign-in cookies	United States
HeyGen	AI avatar videos, presenter voices, and music and sound-effect search	Narration text and audio; scripts	United States
Brandfetch	Fetching public brand logos	Website domain names (no personal data intended)	United States
Slack Technologies, LLC	Internal notifications to Clevera staff, including sign-ups, failed jobs and support messages	Names, email addresses, support messages and job details such as titles	United States

Not Sub-processors. Lemon Squeezy processes payments as Merchant of Record and independent Controller (section 2.5). Services the Customer connects, including the Clevera app for Slack and analytics the Customer adds to its Help Centers, act on the Customer's instructions (sections 3.3(d) and 3.4). Providers that Clevera uses only for data it controls, such as its website analytics, sign-in location lookups and the network services for its website and free tools, are described in the Privacy Policy and at https://www.clevera.ai/subprocessors.