Data Processing Agreement

Coresteads OÜ | Version 0.10 | 19 October 2026

Template to complete for each client. For legal and operational review; not an executed agreement. Complete the square-bracket fields and Annexes A-C, and verify the measures before processing personal data.

1. Parties, roles and scope

1.1 [Client legal name], registry code [code], address [address] ("Controller"), and Coresteads OÜ, registry code 17617785, Varju tee 8, Pirita linnaosa, Tallinn, Estonia ("Processor"), enter into this data processing agreement ("DPA"). Contacts: [client contact] and info@coresteads.com.

1.2 This DPA supplements the Master Service Agreement dated [date] ("Agreement"). If there is no master agreement, the parties' approved statement of work [reference] defines the service scope. Solution means the AI agents, skills, subagent workflows, integrations or scheduled runs described there.

1.3 The Controller determines the purposes and essential means and ensures a legal basis, notices to individuals and lawful instructions. Coresteads processes data on the client's behalf only to provide the agreed service. If Coresteads determines purposes and means itself, its role is assessed separately; website inquiries are covered by the separate privacy policy.

1.4 Annex A specifies the subject, nature, purpose, duration, types of personal data and categories of individuals. Terms follow Regulation (EU) 2016/679 (GDPR). Processing must not begin before the annexes and necessary providers are approved.

2. Instructions and core obligations

2.1 Documented instructions comprise this DPA, the Agreement, the statement of work and later written instructions, including those for transfers outside the EEA. Coresteads informs the client before other processing required by law unless that law prohibits notice. It promptly flags an apparently unlawful instruction and does not perform the disputed operation before clarification.

2.2 Access is limited to authorised persons bound by confidentiality. Coresteads applies Annex C, limits access and data volume, and does not use client personal data for its own purposes or to train its own AI models.

2.3 A model service may be used only on documented instructions with verified commercial terms and settings excluding use of client content for general model training without the client's separate written instruction. Retention, security review and any feedback or abuse-monitoring exceptions are assessed separately before use. No training does not mean no retention.

3. Assistance, sub-processors and transfers

3.1 Coresteads reasonably assists with individual rights and GDPR Articles 32-36, taking account of the nature of processing and information available to it. A directly received request is forwarded without undue delay, no later than five business days; it is not answered on the client's behalf without instructions unless the law requires otherwise. Coresteads maintains required records of processing.

3.2 General written authorisation covers only sub-processors specifically named in Annex B. At least 14 calendar days' notice is given before additions or replacements. The client may object on reasonable data protection grounds within that period; no data is given to a disputed new provider before resolution. If no agreement is reached, the client may terminate the affected statement of work without penalty.

3.3 Coresteads binds each sub-processor in writing to substantively the same data protection obligations and remains responsible to the client for performance of those obligations. A provider contracted directly by the client does not become Coresteads' sub-processor solely because Coresteads configures the service; the actual role, contracting party and instruction chain are recorded in Annex B.

3.4 A transfer outside the European Economic Area, including relevant remote access, requires client instructions and a GDPR Chapter V basis. Standard Contractual Clauses are selected for the actual roles; transfer impacts and supplementary measures are assessed where required. An adequacy decision may be relied on only while valid and where the recipient is covered. A client account or EU database does not establish that the entire data chain stays in the EEA.

4. Security, breaches and audit

4.1 Annex C measures must be appropriate to risk and implemented before processing. They may be updated without reducing protection. The client is informed of changed risks or a material protection gap, and remediation is agreed.

4.2 Coresteads notifies the client of a personal data breach affecting the client's data without undue delay and in any event within 48 hours of awareness. This is a contractual maximum, not permission to delay. Initial notice must not await a complete investigation: it gives the known description, affected data and individuals, likely consequences, contact and measures taken or proposed; information is supplemented promptly.

4.3 The client decides on notification to authorities and individuals and remains responsible for its statutory deadlines. Coresteads preserves relevant evidence and assists with notifications and resolution.

4.4 Coresteads makes available information needed to demonstrate compliance and allows and contributes to audits, including inspections, by the client or its independent auditor. Routine audits are normally planned annually with 30 days' notice; this does not restrict justified additional checks, urgent post-breach checks or authority powers. Reasonable costs and confidentiality are agreed without preventing a lawful audit.

5. Termination, liability and signatures

5.1 On termination Coresteads returns or deletes personal data and existing copies at the client's choice, normally within 30 calendar days unless Annex A specifies a shorter period. Return uses a common machine-readable format; remaining copies are then deleted. Completion is confirmed in writing.

5.2 If law requires retention, the basis and period are recorded, processing is restricted and data is deleted when the duty ends. Backup deletion cycles and access limits are defined in Annex A before processing; backups may not be kept indefinitely or used for ordinary processing. Deletion instructions are reapplied after restoration.

5.3 Liability allocation follows the Agreement without restricting rights of individuals or authorities under the GDPR. This DPA prevails over conflicting provisions concerning personal data; mandatory law and applicable Standard Contractual Clauses remain paramount. Estonian law applies.

5.4 The ET and EN templates are substantively parallel. For bilingual execution, the parties choose the prevailing language: [ET / EN]. This DPA is not itself consent to a new processing purpose.

Signatures

Controller: [legal name, signatory name, role, date, signature]

Processor: Coresteads OÜ; [signatory name, authority, date, signature]

Annex A. Processing details - complete before starting

Statement of work and purpose: [reference; specific business process and authorised result].

Nature and frequency: [reading, classification, extraction, drafting, transfer, deletion; continuous / project only / scheduled].

Individuals and data: [exact categories and fields; sources and systems]. Special category and criminal offence data are excluded unless a separate legal basis and safeguards are agreed here.

Duration and periods: [start/end; purpose and period for working copies and logs; backup deletion cycle]. The proposed log retention maximum is 90 days unless a justified shorter period or another applicable requirement is confirmed here. This is a contractual requirement, not evidence of an existing setting.

Data flow and approvals: [source -> tool -> model service -> output; locations and remote access; actions requiring human approval; client and Coresteads owners].

Annex B. Provider register - complete for each project

No provider is automatically authorised by this blank template. Add each actual sub-processor separately, and identify directly contracted client providers with their distinct role.

Each record must contain: [exact legal name and contact]; [service and data processed]; [Coresteads sub-processor / client's direct processor]; [contract and DPA reference]; [data locations and remote-access countries]; [transfer basis, SCC module and impact assessment where needed]; [retention, deletion and training-use setting]; [approver and date].

Providers to assess where needed may include Anthropic Claude API, Google Workspace or another email/document service, a workflow host and other integrations. These are examples, not authorisations. A product name does not replace the contracting entity's legal name.

The Firebase/Firestore/Resend chain of Coresteads' public website form is not automatically a client project's data chain. If those services are used on a client's behalf, they must be assessed and named separately here.

Annex C. Technical and organisational requirements

These measures are contractual requirements. Record an owner, implementation evidence and exceptions before processing; an unimplemented measure must not be described as an existing safeguard.

1. Access and secrets. Named accounts, least privilege, MFA on supported administration accounts, access reviews and prompt removal when no longer needed. Secrets are held in a dedicated secret store or password manager, not in source code, public prompts or emails.

2. Separation and encryption. Separate client data, configuration and credentials. Use TLS; verify encryption of stored data and work devices and its implementation by providers. Devices have screen locks, security updates and protection appropriate to risk.

3. Minimisation and AI. Use synthetic or anonymous data in development where possible; pseudonymised data remains personal data. Restrict tools and data sources; model output is not a trusted instruction. High-impact sending, payments, access or contract changes require agreed human approval.

4. Logs, recovery and deletion. Log necessary actions, errors, approvals and usage; avoid full content and secrets. Retention follows Annex A. Define and test risk-appropriate backups, recovery checks and availability measures before production use.

5. Tests and incidents. Perform agreed checks before handover and after material changes, including access and restriction tests. Document incident contacts, detection, containment, evidence preservation, notification and remediation. Regularly assess control effectiveness according to risk.