

Data Processing Agreement Template

A free, adaptable customer-facing data processing agreement for a SaaS company acting as processor: ten clauses with filled sample wording, Annexes I to IV, a one-page vendor-side checklist, a changes log, and a customization checklist. Shaped by GDPR Article 28, with notes for UK GDPR and the CCPA.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with a fact about your own product, delete any clause that does not describe your practices, and fill the annexes from the controls and vendors you actually run. Bracketed ranges for notice hours, notice days and deletion windows are examples only. GDPR Article 28 sets none of those numbers: they are commercial terms the parties agree. Have a lawyer read the final version before it goes to a customer.

Processor (Company): [Company legal name]

Customer (Controller):
[Customer legal name]

Master agreement: [Title and date]

Order or service: [Product / service name]

Version: [1.0]

Effective date: [Date]

Security contact (Annex I):
[Email]

Privacy contact: [Email]

Part A: Customer-facing Data Processing Agreement (processor version)

Background and definitions

This Data Processing Agreement ("DPA") forms part of the agreement between [Company] ("Processor") and Customer ("Controller") named above (the "Agreement"). It applies to Personal Data that Processor processes on behalf of Customer in providing the Services. "Customer Personal Data", "Data Subject", "Personal Data Breach", "Processing", "Controller", "Processor" and "Supervisory Authority" have the meanings given in the GDPR. Where Customer is subject to the UK GDPR, references to the GDPR include the UK GDPR. Where Customer is a business under the CCPA, Processor acts as Customer's service provider as described in Clause 11.

Clause 1: Subject matter, duration and description of processing

Processor processes Customer Personal Data only to provide the Services described in the Order, for the term of the Agreement and any period needed to return or delete the data under Clause 8. The nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects are described in Annex I.

Clause 2: Documented instructions

Processor will process Customer Personal Data only on Customer's documented instructions, which are this DPA, the Order, and Customer's use and configuration of the Services. Further instructions must be given in writing, including by email. Processor will not process Customer Personal Data for its own purposes [except: list any agreed product-improvement use, or delete this bracket]. If Processor is required by law to process Customer Personal Data otherwise, it will inform Customer before processing unless that law prohibits it. If Processor believes an instruction infringes applicable data protection law, it will inform Customer immediately and may suspend the affected processing until Customer confirms, amends or withdraws the instruction.

Clause 3: Confidentiality and security

Processor ensures that every person authorized to process Customer Personal Data is bound by a duty of confidentiality. Processor maintains the technical and organizational measures described in Annex II and will not materially reduce the level of protection they provide during the term of the Agreement.

Clause 4: Sub-processors

Customer gives Processor general written authorization to engage the sub-processors listed in Annex III. Processor will inform Customer of any intended addition or replacement at least [15 to 30] days before it takes effect, by [email to the contact in Annex I / notice at the sub-processor page]. Customer may object on reasonable data protection grounds within [10 to 14] days, and the parties will work in good faith to resolve the objection. If the objection cannot be resolved, Customer may terminate the affected Services [without penalty]. Processor will bind each sub-processor to data protection obligations no less protective than this DPA and remains fully liable to Customer for each sub-processor's performance.

Clause 5: Assistance

If Processor receives a request from a Data Subject concerning Customer Personal Data, it will forward the request to Customer within [5 to 10] business days and will not respond except on Customer's instructions. Taking into account the nature of the processing and the information available to it, Processor will give Customer reasonable help to respond to Data Subject requests and to meet Customer's obligations under Articles 32 to 36 of the GDPR, including data protection impact assessments and prior consultation. [Assistance beyond [X] hours per year may be charged at Processor's then-current rates.]

Clause 6: Personal Data Breach notification

Processor will notify Customer without undue delay, and in any event within [24 to 72] hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notice will go to the security contact in Annex I and will describe, as far as known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Where all information cannot be provided at the same time, it may be provided in phases without further undue delay. Customer remains responsible for deciding whether to notify a Supervisory Authority or Data Subjects.

TWO CLOCKS, TWO PARTIES

Article 33(1) gives the controller 72 hours, where feasible, to notify the authority. Article 33(2) tells the processor to notify the controller without undue delay. The hours in this clause are a contractual choice, not a statutory processor deadline.

Clause 7: Information and audits

Processor will make available the information needed to show compliance with this DPA, including [its current SOC 2 or ISO 27001 report] on request. Customer may audit Processor's compliance [once in any 12-month period] on [30] days' written notice, and at any time where a Supervisory Authority requires it or a Personal Data Breach has occurred. Audits will be limited in scope and duration, will respect Processor's confidentiality and security rules, and are at Customer's cost unless the audit finds material non-compliance. Customer may use an independent auditor bound by confidentiality.

Clause 8: Deletion or return

On termination, Customer may by written notice within [30 to 60] days elect to have Customer Personal Data returned in [a standard export format] or deleted. Processor will then delete it from production systems within [30 to 90] days and from backups within [the next backup cycle, not longer than 90 days], and will certify deletion in writing on request. Processor will retain data only where applicable law requires it and will tell Customer which law applies.

Clause 9: International transfers

Where processing involves a transfer of Customer Personal Data to a country that is not covered by an adequacy decision, the parties rely on the transfer mechanism identified in Annex IV. If this DPA conflicts with that mechanism, the mechanism prevails.

Clause 10: Liability, governing law and order of precedence

[Each party's liability under this DPA is subject to the limitations in the Agreement / the following limit applies to data protection claims: ____.] This DPA is governed by [the law that governs the Agreement, or the law of an EU Member State where the transfer mechanism requires it]. In the event of conflict, the transfer mechanism in Annex IV prevails, then this DPA on data protection matters, then the Agreement.

Clause 11: Regional terms (delete if not needed)

California. Processor will not sell or share Customer Personal Data; will process it only for the specific business purposes in Annex I; will not retain, use or disclose it outside those purposes or outside the direct business relationship; will comply with the CCPA and give the same level of privacy protection; will allow Customer reasonable steps to check compliance and to stop and remediate unauthorized use; will notify Customer if it can no longer meet its obligations; will help Customer respond to consumer requests; and will bind any subcontractor to the same terms. **United Kingdom.** Where the UK GDPR applies, the parties rely on [the UK IDTA / the UK Addendum] as identified in Annex IV.

Signature

For Processor	For Customer
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date:

Annex I: Processing details and contacts

Field	Entry (replace the example)
Parties and contacts	[Processor name, address, privacy and security contacts]; [Customer name, address, contact]
Subject matter	Providing the [Product] [service description] service
Duration	The term of the Agreement plus the return or deletion period in Clause 8
Nature and purpose	Hosting, storing, analyzing and displaying Customer-submitted data to deliver the Services
Categories of Data Subjects	Customer's employees, contractors and end users
Types of Personal Data	Names, work email addresses, user IDs, [support ticket content], usage logs
Special categories	None. Customer will not submit special category data without prior written agreement
Frequency	Continuous for the term
Retention	Until deletion or return under Clause 8
Business purposes (California)	[Specific list. Do not write "the Services" alone]

Annex II: Technical and organizational security measures

Write this from what you run. Each row should name a control a reviewer can check, and nothing you do not operate. Keep Annex III identical to your public sub-processor page and vendor inventory.

Area	What to state (replace the example)
Access control	Role-based access, MFA for production, access reviews [quarterly]
Encryption	Encryption in transit and at rest for Customer Personal Data
Logging	Production access and administrative actions logged and retained for [period]
Vulnerability management	Scanning and patching process with named owners
Backup and recovery	Backups [frequency], restore tested [frequency]
Incident response	Documented plan, tested [frequency], named contact
Personnel	Confidentiality commitments; security training at onboarding and [annually]
Vendor management	Sub-processors reviewed before engagement and [annually]

Annex III: Approved sub-processors

Name	Service	Data touched	Location	Transfer mechanism
[Cloud host]	Hosting and storage	All Customer Personal Data	[Region]	[Annex IV / not applicable]
[Email provider]	Transactional email	Names, email addresses	[Region]	[Annex IV / not applicable]
[Support tool]	Support tickets and chat	Ticket content, contact details	[Region]	[Annex IV / not applicable]
[AI or LLM API provider]	Features that process Customer content	Content submitted to the feature	[Region]	[Annex IV / not applicable]

Annex IV: Transfer mechanism pointer

Mechanism: [Adequacy decision / EU standard contractual clauses, Module [Two or Three] / UK IDTA / UK Addendum / not applicable]. Exporter: [name]. Importer: [name]. Date signed: [date]. Notes: [any option choices made, such as governing law and forum]. This Annex names the mechanism only. Which mechanism applies and what assessment sits behind it is a separate decision: see <https://www.complyjet.com/blog/cross-border-data-transfer-requirements>

Part B: Vendor-side checklist (when you are the controller, or a processor engaging a sub-processor)

Use this one-page list before any vendor that touches personal data goes live. It is the same list in reverse: you are the party asking.

Check	
☐	The vendor processes personal data on your behalf (not for its own purposes) and a DPA is signed before any data flows
☐	The DPA covers every Article 28(3) item: instructions, confidentiality, security, sub-processors, data subject requests, Articles 32 to 36 assistance, deletion or return, audits, and the infringing-instruction notice
☐	The annexes describe the real processing and the real security measures, not placeholders
☐	You have the name, address and contact person of every sub-processor, and the vendor will keep them up to date
☐	Sub-processor changes come with notice and a right to object that you can actually use
☐	Breach notice to you is without undue delay, with a stated number of hours you can build your own process around
☐	You know which report the vendor gives you instead of an on-site audit, and how often
☐	Deletion or return at exit is your choice, with a date and a statement on backups
☐	Any transfer outside the EU or UK has a named mechanism in the annex
☐	The vendor cannot use your data to train its own models or for its own purposes unless you agreed in writing
☐	The executed DPA is filed with the vendor record, with version and date

Changes log

Date	Version	What changed	Why	Approved by

Customization checklist

Before you send this to a customer	
☐	Confirm you are the processor for the data in scope, and that no clause lets you use customer data for your own purposes unless you intend it
☐	Fill Annex I from your data map
☐	Fill Annex II from controls you actually run and can show evidence for
☐	Fill Annex III from your vendor inventory and match your public sub-processor page
☐	Choose the transfer mechanism and complete Annex IV, or delete Clause 9 if not needed
☐	Set the bracketed commercial terms: notice hours, notice days, objection days, audit frequency, deletion windows, liability
☐	Delete Clause 11 regions that do not apply
☐	Have counsel review, then sign electronically or by reference and keep the executed copy with the master agreement

This template is a starting point, not legal advice. GDPR Article 28 sets the mandatory contents of a controller-processor contract, but the right commercial terms, liability allocation, governing law and transfer mechanism depend on your product, your customers and the laws that apply to you. Have a qualified lawyer review the final agreement before use. Free to use and adapt. Published by ComplyJet: <https://www.complyjet.com>