Data Processing Agreement

This agreement outlines how biosuite processes personal data on behalf of our customers in compliance with GDPR.

biosuite ApS · Version 1.0 · Effective date: 1 August 2026

This Data Processing Agreement ("Agreement" or "DPA") forms part of the Terms of Service between:

> **biosuite ApS**
>
> Company reg. no. 46609166 (CVR, Denmark)
>
> Copenhagen, Denmark
>
> ("Processor" for Customer Uploaded Data, and separate "Controller" for Platform Usage Data and Account and Billing Data, "we", "us", or "our")

and

> **The Customer using the biosuite Service**
>
> ("Controller", "you", or "your").

This DPA governs our processing of personal data on your behalf when you use the biosuite platform. It is designed to be simple, transparent, and aligned with the GDPR (Regulation (EU) 2016/679).

1. Purpose and scope

What this DPA covers and its objectives

1.1. This DPA applies to the processing of personal data by biosuite ApS on behalf of the Customer in connection with the provision of the biosuite platform and related services ("Service").

1.2. The purpose of the processing is to deliver procurement, spend, and financial workflow features, including document processing, spend analytics, approvals, and data storage.

1.3. The Controller determines the purpose and means of all Customer Uploaded Data (documents and financial records). The Processor determines the purpose and means of Platform Usage Data (logs, security events, device data) as separate Data Controller, solely for security, service operation and improvement, as described in the Privacy Policy.

1.4. Role split: For clarity, biosuite acts as:

- (a) Data Processor for Customer Uploaded Data; and
- (b) Independent Data Controller for Platform Usage Data and for Account and Billing Data processed for security, fraud prevention, service improvement, analytics, contract administration, billing, and compliance purposes.

This role split reflects the nature of the Service and ensures GDPR compliance.

2. Nature of processing, types of data, and categories of data subjects

What data we process and who it relates to

2.1. Nature of processing:

Storage, organization, retrieval, structured presentation, automated optical character recognition and structured data extraction, automated analysis, transmission (including transmission to, and storage in, a dedicated object storage service located in the EU), and deletion of data necessary to operate the Service. The storage locations and the document flow are described in clause 2.4.

2.2. Types of personal data:

Customer Uploaded Data (Processor role):

- Uploaded invoice files and other document files uploaded by the Controller, held in the object storage service described in clause 2.4
- Structured data extracted from those documents, and other financial and procurement records, held in the core application environment
- Personal data contained within such documents

Platform Usage Data (Controller role):

- IP addresses, device identifiers, logs, analytics events
- Security events and diagnostic data
- Account metadata (role, login timestamps, feature usage)
- Account and Billing Data: registration details, contact information, billing address, VAT ID, and subscription and payment records processed for biosuite's own contract administration, accounting, and legal compliance

2.3. Categories of data subjects:

- Customer personnel using the Service

- Vendors, suppliers, and business partners appearing in uploaded financial documents
- Other individuals whose data is included in documents or records uploaded by the Controller

The Processor does not control the content uploaded by the Controller.

2.4. Storage locations:

Uploaded invoice files provided by the Controller are transferred directly from the user's browser to a private object storage service configured with European Union jurisdiction, operated by the sub-processor identified for that purpose in Section 5. The files are not routed through or stored in biosuite's core application environment.

Structured data extracted from those documents, together with account, workspace, and usage data, is stored in the application database hosted in the EU.

For AI-assisted invoice reading, the AI sub-processor retrieves the document from the object storage service by means of a time-limited, access-controlled retrieval mechanism, for the sole purpose of performing the requested extraction. The AI provider's response is received and validated by a server-side function in the core application environment. That response includes the document's recognised text alongside the structured fields; only the approved fields are retained, and the recognised text is neither logged nor stored.

Contract files uploaded for AI contract reading are processed transiently for extraction only and are not retained after extraction.

Access to uploaded invoice files is restricted through server-side access controls.

Further detail on AI processing is set out in the AI Data Processing Policy.

3. Processor obligations

Our commitments regarding data processing

Unless otherwise specified, "personal data" in this section refers to Customer Uploaded Data processed in our role as Data Processor.

3.1. Processing on instructions

We process personal data only on documented instructions from the Controller, including this DPA and the Terms of Service.

3.2. Confidentiality

We ensure that all persons authorized to process personal data are under confidentiality obligations. Access is strictly limited and only granted when necessary to operate or support the Service.

3.3. Security measures

We apply appropriate technical and organizational measures, including those provided by our infrastructure partners, to safeguard your data. These measures include:

- Encryption in transit (HTTPS/TLS) and at rest
- Access controls
- Infrastructure-level monitoring and protections provided by our hosting partners
- Routine, automated backups of the application database performed by our cloud platform provider, and durable, redundant object storage provided by our document storage provider; neither is a customer-facing backup or archiving service, and the Controller remains responsible for retaining its own copies of business-critical documents
- Storage of uploaded invoice files in a private, non-public object storage service configured with EU jurisdiction, separate from the core application environment, with access granted only after server-side verification of the user's identity, company membership, and permissions
- Storage and AI provider credentials are not accessible from the browser, and access is managed on a least-privilege, need-to-know basis
- Automated extraction limited to a defined field schema that excludes bank account numbers and IBANs, SWIFT/BIC codes, payment card data, and payment references
- Automated length limits and filtering of AI-extracted free-text values to reduce the risk that bank or payment identifiers are stored
- Logging practices designed to exclude document content, extracted document text, and access credentials

No method of storage or transfer is completely secure, but we rely on reputable infrastructure providers with industry-standard protections.

3.4. Assistance

We assist the Controller in fulfilling GDPR obligations related to:

- Data subject rights
- Security of processing
- Notification obligations in the event of a breach
- Data protection impact assessments (if relevant)

3.5. Personal data breach

If we become aware of a personal data breach affecting the Controller's personal data, we will notify the Controller without undue delay after becoming aware of the breach, taking into account the information made available to us by our infrastructure providers.

3.6. Deletion

Upon termination of an account, we delete or anonymize personal data following the timelines described in our Terms of Service and Privacy Policy, except where retention is required by law. Deletion covers both the structured data held in the application database and the original documents held in the object storage service. Where the Controller deletes an invoice within the Service, the invoice and its document are immediately removed from all views, reports and totals, and the original document is no longer accessible through the Service unless the invoice is restored. The document remains in the object storage service for 30 days so that a company administrator can restore the invoice, after which the document and the associated invoice fields are automatically and permanently deleted. A record of the deletion is retained. Prior to deletion, the Controller may export the structured records held in the application database using the Service's standard export functionality, and may download original document files from the Service.

4. Controller obligations

Your responsibilities as data controller

4.1. The Controller is responsible for ensuring a lawful basis for all personal data uploaded or processed in the Service.

4.2. The Controller may not upload data that violates applicable laws or infringes third-party rights.

4.3. The Controller is responsible for handling data subject requests except where the Processor is required to assist under this DPA.

4.4. The Controller must not upload restricted data as defined in Section 2.7 of the Terms of Service, which applies to all uploads under this DPA.

4.5. The Controller acknowledges that ordinary supplier invoices may contain the supplier's bank or payment account details as part of the document itself, and that such details remain part of the stored source document. The Processor does not extract, index, or otherwise process such details as structured data, and the Service does not process, initiate, or otherwise contribute to payments. The Controller remains responsible for determining whether its upload of such documents is lawful and appropriate under its own policies and applicable law.

5. Sub-processors

Third parties that help us deliver the Service

5.1. The Controller authorizes the Processor to use the sub-processors listed below. These sub-processors process personal data solely to provide the Service and under written agreements ensuring GDPR-compliant protections. The listed sub-processors may engage their own sub-processors (such as cloud infrastructure providers) under equivalent data protection obligations. An overview of such providers is available upon request.

5.2. The Processor will notify the Controller (by email or in-app notice) at least 30 days before adding or replacing a sub-processor. The Controller may object on reasonable data protection grounds within 14 days of such notice. If the objection cannot be resolved, the Controller may terminate the affected Service as its sole remedy.

Approved sub-processors

Name	Location	What they help us with
September Development ApS	Denmark (EU)	Developing the biosuite platform, with access to personal data as needed to perform these tasks
Cloudflare, Inc.	USA (company) – object storage configured with EU jurisdiction	Storage of uploaded invoice documents in a private object storage bucket (Cloudflare R2, EU jurisdiction); securing our website and speeding up delivery
Mistral AI SAS	France (EU) – certain sub-processors may be located outside the EU/EEA	AI-based document reading (OCR) and structured extraction of invoice data
Lovable Labs Incorporated	USA (Delaware) / Sweden – customer data hosted in the EU region	Hosting, database, authentication, notifications, and AI gateway services. Uploaded invoice documents are not stored on this platform.
Alunta.com ApS	Denmark (EU)	Invoicing, subscription billing, payment administration, and related billing operations
Visma Dinero ApS	Denmark (EU)	Accounting and related financial record-keeping

Name	Location	What they help us with
Oneflow AB	Sweden (EU)	Sending, tracking, and collecting signatures on customer-facing legal documents under clause 9.10 of the Terms of Service
Microsoft Corporation	USA (EU data residency for our tenant)	Business email (Outlook) and office apps

5.3. International transfers outside the EU/EEA are conducted using appropriate safeguards such as Standard Contractual Clauses (SCCs), encryption, and minimized data exposure, as described in our Privacy Policy.

5.4. For information about how biosuite processes data using AI features, see our AI Data Processing Policy. That policy applies to the AI-assisted features described in it. Automated reading of uploaded invoice documents forms part of the standard document workflow; the other AI features apply only where they have been activated or expressly requested within the platform.

6. International data transfers

How we handle cross-border data transfers

6.1. Personal data may be transferred outside the EU/EEA when necessary for the Service, including through the sub-processors listed above and through sub-processors engaged by those sub-processors. This includes sub-processors engaged by our AI document-reading provider, which is established in the European Union but may use its own sub-processors located outside the EU/EEA. Uploaded invoice documents are stored in an object storage bucket configured with European Union jurisdiction. The Processor does not represent that the Service involves no processing outside the EU/EEA.

6.2. The Processor ensures that any such transfer complies with GDPR requirements and provides a level of protection essentially equivalent to that of the EU.

6.3. References to the GDPR in this DPA include, where applicable, the UK GDPR and the Swiss Federal Act on Data Protection (FADP). Transfers of personal data originating from the UK or Switzerland are protected by the Standard Contractual Clauses supplemented by the UK International Data Transfer Addendum or Swiss-specific amendments, as applicable.

7. Audit rights

Your right to verify our compliance

7.1. The Controller may request documentation demonstrating our compliance with this DPA.

7.2. Audit rights are primarily satisfied through written documentation and available certifications or audit reports from our infrastructure providers. Where the Controller reasonably requires further verification under Article 28(3)(h) GDPR, the Controller may conduct (or mandate an independent auditor to conduct) an audit no more than once per 12-month period, upon at least 30 days' written notice, during normal business hours, at the Controller's own cost, and in a manner that does not disrupt Service operations.

8. Liability

Limitations on liability under this agreement

Liability under this DPA follows the limitations set out in the Terms of Service. This DPA does not create additional liability beyond what is stated in the Terms.

9. Term and termination

Duration and ending of this agreement

9.1. This DPA remains in force for as long as the Processor processes personal data on behalf of the Controller.

9.2. Upon termination of the Service, the Processor will delete or anonymize data in accordance with our Privacy Policy and the retention periods described therein. Prior to deletion, the Controller may export the structured records held in the application database using the Service's standard export functionality, and may download original document files from the Service.

10. Acceptance of this DPA

How this agreement becomes binding

This Data Processing Agreement ("DPA") forms part of the Terms of Service between the Customer and biosuite ApS.

This DPA becomes binding when the Customer creates a company workspace within the Service and expressly accepts this DPA through the acceptance step provided during the company creation process.

The Customer must accept this DPA before submitting or storing any personal data within the Service.

The creation of an individual user account without creating a company workspace does not constitute acceptance of this DPA.

By accepting this DPA, the Customer confirms that it acts as Data Controller with respect to any personal data uploaded to the Service.

biosuite ApS may update this DPA from time to time. Where changes materially affect the Customer's rights or obligations, biosuite ApS will provide reasonable notice. Continued use of the Service after such notice constitutes acceptance of the updated DPA, unless the Customer objects before the changes take effect and ceases use of the Service.

11. Effective date

When this agreement takes effect

This DPA becomes effective on the date the Customer expressly accepts it during company workspace creation in the Service.

12. Governing law

Legal jurisdiction for this agreement

This DPA is governed by the laws of Denmark. Any disputes shall be resolved in the courts of Copenhagen, Denmark.

13. Contact

How to reach us about data protection

For questions regarding this DPA or data protection matters, please contact us at hello@biosuite.io or through the contact form on our website.