

Privacy Policy

Your privacy is important to us. This policy explains how we collect, use, and protect your personal information.

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

Thank you for choosing **biosuite** to manage your procurement, spend, and financial workflows. We are committed to protecting your privacy to the best of our ability. This Privacy Policy explains what personal data we collect, how we use and protect it, and your rights regarding this information.

When we say "**Company**", "**we**", "**us**", or "**our**", we mean **biosuite ApS** (company reg. no. 46609166), a company registered in Copenhagen, Denmark. "**Service**" or "**Platform**" refers to our web application and related websites, APIs, and services. "**You**" refers to the individual or company using our Service.

This Privacy Policy describes how we process personal data when you use biosuite or interact with our website. We process personal data in accordance with applicable data protection laws and implement appropriate technical and organizational measures to support such compliance.

This Privacy Policy covers data collected both from logged-in platform users and from visitors to our public website.

biosuite acts as Data Processor for Customer Uploaded Data and as independent Data Controller for Platform Usage Data and for Account and Billing Data.

1. Personal data we collect

Types of information we collect and how we collect it

We collect personal data to provide and improve our Service. This information is collected when you create an account, use the platform, interact with our site, or communicate with us. The types of data we collect include:

- **Account information:** When you register or use biosuite, we collect information such as your name, business or company name, business email address, and a password (which is stored in hashed form). We may also record your role or user type within your organization and any preferences or profile information you provide.
- **Uploaded documents and content:** Our platform allows you to upload documents and data (e.g. invoices, contracts, purchase orders, receipts, and other financial or procurement records). These documents may contain personal or business

information about you and third parties (such as names, signatures, contact details of vendors or partners). We process this content to provide the Service's functionality (for example, to extract invoice data or enable spend analysis). Invoices and other supporting documents are retained in your workspace together with any extracted data you review, confirm, and save. Contracts uploaded for AI contract reading are processed transiently for extraction only: the source contract file is deleted after extraction and is not stored in your workspace; only the extracted contract data that you review, confirm, and save is retained. Uploaded invoice files are transferred directly from your browser to a dedicated object storage service located in the European Union; they are not stored on the core application environment. The structured invoice fields that you review, confirm, and save are stored in the application database. Supplier bank or payment account details that happen to appear on an invoice remain part of the stored source document and are not retained, indexed, or stored as structured data. Free-text values extracted from an invoice, such as descriptions and line item text, are length-limited and automatically filtered for bank and payment identifiers before storage. We treat all uploaded documents as confidential and only process them as needed to deliver the Service (see Section 4 on Security and Section 5 on Sub-processors).

- **Transactional and payment data:** If your company subscribes to a paid plan, we may collect billing details such as your company's billing address, VAT ID (if applicable), and payment information. **Note:** For credit card or payment processing, we use trusted third-party payment processors, so we generally do not store your full payment card details ourselves. We do keep records of your subscription plan, payment transactions, and invoices for accounting purposes (managed via Alunta.com and our accounting provider).
- **Usage data:** We automatically collect data about how you interact with our Service. This includes log data like the dates and times you log in, features or pages you use, the IP address and device information (browser type, operating system) from which you access the Service, and other usage metrics. We collect this information to help administer and secure the platform, and to understand and improve how users use biosuite. For example, we may log actions like when you upload a document or approve a purchase order, and we collect analytics on which features are most used. This usage data helps us troubleshoot issues and optimize user experience.
- **Cookies and similar technologies:** When you visit our website or platform, we use cookies and similar tracking technologies to collect certain data (see Section 3 below for details). This may include your preferences, browser information, and analytics data about your interactions with our site.

- **Communications:** If you contact us (for example, via a contact form, support chat, or email), we will collect the information you provide in those communications (such as your name, email, and the contents of your message or attachments). We use this information to respond to you and keep records of support requests.

We collect the above information either directly from you (e.g., via forms you fill out or data you input on the platform) or automatically through your use of the Service (e.g., via technical logging systems and cookies).

2. How we use your personal data

Purposes for which we process your information

biosuite processes Customer Uploaded Data solely as a Data Processor on behalf of the Customer.

biosuite processes Account and Billing Data and Platform Usage Data as an independent Data Controller for security, service operation, analytics, and product improvement.

We use your personal data solely for legitimate business purposes and as necessary to provide you with our Service. Specifically, we use the information we collect to:

- **Provide and maintain the Service:** We process your data to create and manage your account, authenticate you when you log in, and operate the core functionalities of biosuite. For example, we use your Account Information to identify you and provide you access, and we process the content of your uploaded invoices or contracts to extract data and present it back to you through the platform's features. We also use data to monitor the performance of the Service and ensure it is working as intended.
- **Perform procurement and financial workflows:** The platform uses your data (including documents and transaction details) to help manage your procurement, spending, and financial workflows. This means, for instance, using invoice data you upload to generate spend reports or using contract details to track commitments. All such processing is done to fulfill the purpose of the Service to you and your organization.
- **Communicate with you:** We use contact information (like your email address) to send necessary communications. This includes sending verification emails, password reset messages, notifications about transactions or workflow events (e.g., approvals needed, confirmations), updates about new features or changes to the Service, and responses to support inquiries. We may also send you informational or educational content about using biosuite. We will not send you marketing emails unrelated to the Service without your consent, and you can opt out of non-essential communications at any time.

- **Improve and develop our services:** We may use aggregated, anonymized data derived from your usage to understand how our customers use biosuite and to improve our platform. For example, we analyze overall usage patterns, common feature requests, or performance metrics to make informed decisions about new features or enhancements. Any analytics or research we conduct will not identify you personally or expose any sensitive content of your documents. We also use error logs and usage data to debug and enhance the reliability and security of the Service.
- **Billing and account management:** For customers on paid plans, we use personal data to handle subscription management and billing. For example, we use your provided payment and contact details to send invoices, process payments, and manage renewals or changes to your subscription. We may also notify you of any pricing changes or account status issues (such as failed payments or expiring subscriptions).
- **Security and fraud prevention:** We process certain data (like IP addresses, device info, and usage logs) to protect the security of the platform, our users, and their data. This includes monitoring for suspicious or unauthorized activities, enforcing our Terms of Service (e.g., investigating potential misuse or violations), and taking action against fraudulent or malicious behavior. These measures help keep your account and data safe.
- **Legal compliance:** We may use and retain your data as necessary to comply with our legal obligations. For instance, we keep transaction records for accounting and tax purposes, and we may process personal data to comply with export control laws, respond to lawful requests by public authorities, or fulfill any other legal requirements applicable to our business. If we are required by law to disclose your data (for example, due to a court order or governmental request), we will do so only to the extent necessary and, when permitted, we will inform you of such disclosures.

We rely on various legal bases under the GDPR for processing personal data. Most of our processing is necessary to perform the contract between you (as a user or customer) and us (by providing the Service and its features). In some cases, we process data to comply with a legal obligation or because it is in our legitimate interest (such as improving our Services or ensuring security). If we rely on your consent (for example, for certain optional cookies or marketing communications), we will explicitly obtain it, and you have the right to withdraw that consent at any time.

For Platform Usage Data, biosuite is the Data Controller and relies on legitimate interest (GDPR Art. 6(1)(f)) for security, fraud prevention, diagnostics, and service improvement.

No selling of personal data: We **never** sell, rent, or trade your personal information to third parties for their own commercial use. We also do not share the contents of your uploaded documents or records with any third party except as needed to provide the Service (for example, with a sub-processor as listed in Section 5, or when you choose to integrate a third-party service) or as required by law. In plain terms: **your data stays your data**, and we use it only to run and improve biosuite for you.

3. Cookies and tracking technologies

Use of essential cookies

We only use cookies and similar technologies that are strictly necessary for the operation and security of the biosuite platform. These include:

- **Session cookies**, which keep you logged in as you navigate the platform
- **Security and performance cookies**, for example those set by our infrastructure providers (such as Cloudflare) to protect the site against abuse and ensure reliable delivery
- **Preference cookies**, such as language settings, where applicable

We do not use marketing cookies or cookies for user profiling.

We also do not use analytics cookies that require consent under EU law.

Some of our service providers may use cookies that are strictly necessary for the service they deliver (for example, load balancing or security). These cookies do not collect information for advertising or cross-site tracking.

If you have questions about our technical setup or cookie usage, you are welcome to contact us (see Contact Information below).

4. Data storage and security

Where we store data and how we protect it

We understand that the data you entrust to biosuite is often sensitive (financial and business information), and we apply appropriate technical and organizational measures, including those provided by our infrastructure partners, to safeguard your data.

- **Data hosting location:** Our application infrastructure, including the application database and its backups, is hosted by our cloud platform provider (see the sub-processor list in Section 5) in the European Union. Uploaded invoice files are stored separately, in a private object storage bucket operated by Cloudflare (Cloudflare R2) and configured with European Union jurisdiction, which means the stored objects are held in the EU and are reachable only through the corresponding EU endpoint. The

storage service is not publicly accessible, and access to uploaded invoice files is restricted through server-side access controls and appropriate technical and organisational security measures. Automated reading of invoice documents is performed by an AI provider established in the European Union. (In Section 5 below, we list the specific sub-processor services that host or handle data on our behalf, including where a provider is incorporated outside the EU or may itself process data outside the EU.)

- **International access and transfers:** We serve users across various countries, including outside Europe, such as the United States. If you are accessing the Service from outside the EU, be aware that your personal data will be transferred to and stored in the EU. Additionally, some of our sub-processors or service providers may process data outside the EU. In all cases, we ensure that any transfer of personal data out of the EU is done in compliance with GDPR – for example, by implementing the European Commission's Standard Contractual Clauses (SCCs) or other appropriate safeguards. Our goal is to ensure your data enjoys the same level of protection no matter where it's accessed or processed from.

When using sub-processors located outside the EU/EEA (such as Cloudflare or AI service providers), personal data may be processed in those jurisdictions solely for the purpose of delivering the relevant functionality. We only transfer the minimum data necessary for each service, and we apply additional technical and organizational measures to protect the data during transfer (including encryption in transit and strict access controls).

Our AI document-reading provider is established in the European Union, but it may engage its own sub-processors located outside the EU/EEA for parts of its service. We therefore do not represent that all processing takes place exclusively within the EU/EEA.

References to the GDPR in this Policy 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.

- **Encryption in transit and at rest:** We protect data in transit between your device and our servers by using encryption protocols such as HTTPS/TLS. This means that when you send or receive information via our Service, it is encrypted so that no one can intercept and read it. We also encrypt data at rest on our servers and databases. In practice, this includes encrypting the database storage and any backups. These measures protect your data from unauthorized access both as it travels over the internet and when it is stored on disk.

- **Security measures:** biosuite implements industry-standard security practices to safeguard personal data. This includes firewalls and network security measures to protect our infrastructure, access controls to ensure only authorized personnel and sub-processors can access data (and only on a need-to-know basis), and regular security training for our team. Uploaded invoice files are held in a private object storage service that is not publicly accessible. Access is restricted through server-side access controls and appropriate technical and organisational security measures. Our cloud platform provider performs **routine, automated backups** of the application database as part of its managed services, and our document storage provider provides durable, redundant object storage. We rely on both to help prevent data loss, but neither is a customer-facing backup or archiving service, and we recommend that you retain your own copies of any documents that are important to you. Our infrastructure providers include monitoring and alerting capabilities that help detect potential security issues, and we make use of these to maintain the security of the Service. If we ever experience a data breach that affects your personal data, we will notify you and the relevant authorities as required by law. However, no method of transmission or storage is completely secure. While we strive to protect your personal data to the best of our ability, we cannot guarantee its absolute security.
- **Confidentiality:** We consider the content you upload (invoices, contracts, etc.) to be **confidential**. Our team will not access or view your uploaded documents or personal data unless it's necessary to support you or operate the Service (for example, if you request troubleshooting help that requires our engineers to investigate a data issue, or if our automated systems process a document). In practice, automated processes handle most document processing. Access to customer documents is strictly limited and, when necessary, logged in accordance with our platform capabilities. We will not disclose your confidential information to any third party except as described in this Policy (e.g., with our sub-processors or if required by law).
- **Data retention:** We retain your personal data only for as long as necessary to fulfill the purposes outlined in this Privacy Policy or as required by law. In general, for as long as you have an active account with us, we will keep your information on our systems so we can provide the Service. If you choose to delete your account or if your subscription ends, we will initiate deletion of your personal data from our production systems after a defined retention period. Specifically, we typically retain account data for a short grace period in case you reactivate your account or in the event it was accidentally deleted. After this period (generally around 30 days), we aim to permanently delete or anonymize personal data associated with your account within the capabilities of our platform and infrastructure providers. Deletion covers both the structured data held in the application database and the original documents held in the object storage

service. When you delete 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. Some data may be retained in database backups for a slightly longer period before those backups are rotated out; however, if we restore a backup, we will not re-introduce data for accounts that have been deleted. Additionally, we may keep certain information for a longer duration if necessary for legal compliance or legitimate business purposes – for example, we might retain payment records, invoices, or audit logs for a period required by financial regulations or tax laws. Any such retained data remains subject to this Privacy Policy and applicable law.

- **Your GDPR rights:** You have the right to request access to your personal data, request correction, deletion, restriction of processing, and data portability. You may also object to certain processing, withdraw consent where applicable, and lodge a complaint with a supervisory authority – in Denmark, Datatilsynet (www.datatilsynet.dk). To exercise any of these rights, please contact us (see Section 7: Contact Us). We may need to verify your identity before handling your request. Some rights may be limited by legal or contractual requirements.

5. Data sharing and sub-processors

Third parties assisting us (and no unauthorized sharing)

We do not disclose your personal data to third parties **except** in the following cases: (a) to our trusted service providers (sub-processors) that help us run the Service, (b) if you explicitly integrate or instruct us to share data with a third-party service, or (c) when we are legally compelled to do so. We **never sell** your personal data to anyone. When we do share data, we ensure it is protected and only used for the intended purpose.

Sub-processors: The following are the key sub-processor services that biosuite uses to deliver its functionality. These third-party partners may handle or process certain personal data on our behalf, under strict confidentiality and data protection agreements:

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
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

We engage each of these providers under terms (such as Data Processing Agreements or equivalent arrangements) that include commitments to confidentiality, security measures, and compliance with GDPR or equivalent data protection frameworks. We will update this Privacy Policy if we add or change any significant sub-processor. If you have questions about any specific provider or our data-sharing practices, feel free to reach out to us.

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.

Other sharing: In addition to the sub-processors, we may share information in a couple of other scenarios:

- If **you request or consent** to us sharing data with a third party. For example, if biosuite offers an integration with a third-party accounting system and you choose to enable it, we will transfer data to that third party as needed to fulfill the integration, but only with your authorization.
- If required by **law or lawful request**: If a court, law enforcement agency, or regulatory authority with jurisdiction over us requests certain data, we may be obligated to comply. In such cases, we will only provide the minimum data necessary and, if the law allows, we will inform you of the request. Similarly, if needed to enforce our Terms of Service or to protect our rights or the rights and safety of others, we might disclose information to legal advisors or authorities.
- In the event of a **business transfer**: If biosuite (the company) is involved in a merger, acquisition, or sale of all or a portion of its assets, your data may be transferred to the new ownership as part of that deal. If that happens, we will endeavor to ensure the successor adheres to equivalent privacy commitments as stated here, and we will notify you of any significant changes in how your data is handled.

Crucially, aside from the situations described above, **we do not share your personal data with third parties**. We do not provide your information to advertisers, we do not sell user lists, and we do not monetize your data in any way outside of providing you the Service. Our business model is subscription-based, and not dependent on exploiting user data. Your trust is important to us, and we protect your data accordingly.

6. Changes to this Privacy Policy

Updates and how we notify you

We may update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or the features of our Service. If we make a significant change, we will notify you by appropriate means – for example, by emailing the primary account contact, or by placing a prominent notice in the biosuite application. We will also update the "Last updated" date at the top of this Policy.

Please review this Policy periodically to stay informed about how we protect your data. Continuing to use biosuite after a revised Privacy Policy has become effective signifies that you have read and understood the latest version of the Policy. If we propose to use your personal data for a new purpose not covered by this Policy, we will obtain your consent where required by law.

7. Contact us

Questions, requests, and communications

If you have any questions or concerns about this Privacy Policy or about how biosuite handles your personal data, please reach out to us. We are here to help and address any issues you might have. You can contact us by email at **privacy@biosuite.io**.

For privacy-specific inquiries (e.g., questions about data protection, requests to exercise your rights, reports of security incidents), please include the subject line "Privacy Inquiry" or "GDPR Request" as appropriate, and provide detail about your request. We will respond as soon as possible, and no later than required by law.

We value your privacy and trust. Thank you for using biosuite, and please don't hesitate to contact us if you need any clarification or assistance regarding your personal data.