PharmaLCA – Information Security Q&A

October 2026

About this document

This document sets out how AllocNow GmbH protects PharmaLCA and the data our customers entrust to it. It answers the questions that organizations most often ask in their information security and procurement assessments, so that security and IT teams can complete their review quickly.

All statements reflect AllocNow's Information Security Management System (ISMS), which is certified to ISO/IEC 27001:2022. Supporting evidence, such as the ISO/IEC 27001 certificate, can be provided on request (see *Contact for security inquiries*).

Company and product overview

Who provides PharmaLCA?

PharmaLCA is developed and operated by AllocNow GmbH, a software company headquartered in Germany.

Company details	
Legal entity	AllocNow GmbH
Registered address	Friedrich-Ebert-Strasse 17, 53177 Bonn, Germany
Commercial register	District Court of Bonn, HRB 26540
VAT ID	DE347326705

What is PharmaLCA?

PharmaLCA puts life cycle assessments (LCA) within reach of the entire pharmaceutical value chain. It is the LCA software for PAS 2090, the first sector-specific LCA standard for pharmaceuticals. The web-based platform requires no installation and guides users through end-to-end product assessments covering all 16 impact categories of the European Commission's Product Environmental Footprint (PEF) method. It serves drug manufacturers, smaller pharmaceutical companies, contract manufacturers, suppliers and sustainability professionals, regardless of their LCA experience. PharmaLCA was launched on October 6, 2026, at CPHI Milan.

Who was PharmaLCA developed with?

PharmaLCA was developed by AllocNow in collaboration with the Pharma LCA Consortium, which endorses the software. The consortium was launched in November 2023 under the Pharmaceutical Environment Group, with support from the Sustainable Markets Initiative's Health Systems Task Force. Its members are:

AstraZeneca · Chiesi · GSK · Johnson & Johnson · Merck KGaA · MSD · Novartis · Novo Nordisk · Pfizer · Roche · Sanofi · Takeda

Has PharmaLCA been independently evaluated?

Yes. The software has successfully undergone an independent evaluation by TÜV SÜD based on the requirements of PAS 2090.

Which plans are available, and which security-relevant features do they include?

PharmaLCA is offered in two plans. The security controls described in this document apply to both plans unless stated otherwise.

Feature	Starter (free)	Professional
Unlimited modeling No limits, no surprises. Build unlimited models across every life-cycle stage — so cost never stands between you and the next assessment.	☑	☑
PAS 2090 Guidance The standard, built into every step. PharmaLCA turns PAS 2090 into guided questionnaires and defaults — compliant assessments, no expertise required.	☑	☑
Hotspot analysis & results drill-down Find the hotspots, not just the number. Drill into any life-cycle stage to see which materials and processes drive impact — and where to act first.	☑	☑
Custom PDF report generation Share results, not spreadsheets. Generate a clean, PAS 2090-aligned PDF from any finished model — ready for partners, customers, or auditors.	☑	☑
BAFU database Real impact data, built in. Start modeling with the open-source BAFU database included from day one — no separate license, no extra cost.	☑	☑
ecoinvent database Premium data for serious assessments. A curated, pharma-relevant subset of ecoinvent, with full LCIA scores — the depth and quality that stand up to scrutiny.	—	☑
Carbon Minds cm.chemicals database Built for chemicals. Add the Carbon Minds cm.chemicals database — specialized, high-quality factors for the chemical inputs behind pharmaceutical products.	—	Add-on
Multi-user collaboration (Spaces) Your team, one workspace. Spaces let colleagues collaborate on the same models — shared context, shared progress, no version chaos.	—	☑
Single sign-on (SSO) One login, company-wide. Enforce SSO across your tenant so every user signs in through your existing identity provider.	—	☑
Backup, Bulk Export, Data Recovery Never lose an assessment. Built-in backup, one-click bulk export, and data recovery protect the work your team depends on.	—	☑
Full data privacy Your data is never used for AI training, analytics, or any other secondary purpose — stored and processed for one reason only: your assessments.	—	☑

Information security management and ISO certification

Is AllocNow certified to ISO/IEC 27001?

Yes. AllocNow GmbH operates an Information Security Management System (ISMS) certified to ISO/IEC 27001:2022. The certification audit was carried out by RSM Certification GmbH.

What does the ISMS cover?

The ISMS covers all of AllocNow's core business processes and the IT systems and applications that support them. This includes software development, customer onboarding, customer service, supplier management and the AWS cloud infrastructure on which PharmaLCA runs. As AllocNow has no physical offices or data centers, physical security of the hosting infrastructure is provided by our cloud provider and verified through its certifications.

How is the ISMS maintained and reviewed?

- A Statement of Applicability covers all 93 controls of ISO/IEC 27001:2022 Annex A.
- An internal audit is conducted annually, following a rolling three-year audit program.
- Management reviews the ISMS at least once a year.
- Information security risks are recorded in a risk register and reviewed regularly.
- The Information Security Policy and the ISMS are reviewed at least annually, or after significant changes, incidents or audit results.

Which certifications does the hosting provider hold?

Our hosting provider, Amazon Web Services (AWS), is certified to ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 and holds SOC 2 reports covering the services used to host PharmaLCA.

Policies, organization and people security

Which information security policies are in place?

AllocNow's Information Security Policy is approved by management and aligned with ISO/IEC 27001:2022. It is supported by topic-specific policies, including:

- Information Classification and Labeling Policy
- Cloud and SaaS Management Policy
- Supplier Management Policy
- Business Continuity Policy
- Data Retention Policy
- Cryptography Policy

Who is responsible for information security?

The Management Team of AllocNow owns information security and approves the Information Security Policy. Management has appointed an Information Security Officer, who maintains the ISMS, and a Data Protection Officer, who ensures compliance with the GDPR.

How are employees made aware of their security responsibilities?

- Every new employee completes a mandatory security onboarding.
- Employees take part in regular security awareness training.
- Employees are bound by confidentiality obligations that continue after employment ends.

How are company devices secured?

All company devices are centrally managed and must meet a security baseline: an up-to-date operating system, anti-malware protection and full-disk encryption.

Hosting, infrastructure and encryption

Where is PharmaLCA hosted?

PharmaLCA is a fully managed SaaS application hosted on Amazon Web Services (AWS) in Frankfurt, Germany. Application data remain in the EU. AllocNow operates, maintains and patches the platform.

How is customer data separated between companies?

Each customer company is a separate tenant with its own dedicated database. Access is limited to the tenant's own users and to authorized AllocNow operations staff (see *Access control and authentication*).

Are development, test and production separated?

Yes. Development, quality and production environments are separated, each with its own databases and user pools. Customers use the production environment. Production data is never copied to development or test environments.

Is data encrypted?

- In transit: HTTPS only, with TLS 1.2 or higher. Older protocols are disabled.
- At rest: databases, backups and file storage are encrypted with AES-256, with keys managed in AWS Key Management Service.
- Credentials and secrets are kept in a dedicated secrets management service and never stored in plain text.
- Only certificates from publicly trusted certification authorities are used.

How is the application protected against attacks from the internet?

- The application and its API are protected by a web application firewall with managed rule sets.
- Security-relevant activity is logged and monitored.
- Network and firewall changes are made only through peer-reviewed changes to code.
- Sign-in and registration forms are protected against bots.
- Customers who want to run their own vulnerability scans can do so after prior written agreement.

Does PharmaLCA need to connect to customer systems?

No. PharmaLCA is used in the browser; nothing is installed on customer devices or servers. It runs in current Chromium-based browsers (for example Chrome and Edge) and is designed for desktop use.

- The only network traffic needed is outbound HTTPS (TCP 443) from users' browsers to app.pharmalca.com and to Cloudflare Turnstile. There are no inbound connections to customer networks.
- PharmaLCA has no external API or interfaces to customer systems. Results are exported by users as Excel files and PDF reports.
- System emails, such as email verification and password resets, are sent via AWS from the PharmaLCA sender domain, which is configured with SPF, DKIM and DMARC.

Access control and authentication

How do customer users sign in to PharmaLCA?

Authentication is based on the OpenID Connect (OIDC) and OAuth 2.0 standards. Each user account is the user's business email address. Two options are available:

- Single sign-on (Professional plan): the customer's identity provider, for example Microsoft Entra ID or Okta, is connected via OpenID Connect. For Entra ID, PharmaLCA uses delegated sign-in permissions only; it requests no application permissions and has no access to other resources in the customer's tenant.
- Password sign-in: users sign in with their business email address and password, and multi-factor authentication (authenticator app) is mandatory. Passwords are never stored in plain text.

Who can register for a company's tenant?

Users are assigned to their company's tenant by their email domain. Users from approved company domains can register directly; registrations from unknown domains are held for manual review by AllocNow before access is granted.

How are sessions protected?

- Sessions are managed server-side and expire after one hour. SSO users always sign in through their company's identity provider.
- Access tokens are never exposed to the browser, which only holds a secure session cookie.
- Sign-in flows follow current OAuth 2.0 security best practice.

Can access be restricted within a customer's tenant?

Yes. PharmaLCA uses role-based access. The customer's Subscription Owner(s) manage seats and roles, and work is organized in Spaces with moderators and collaborators. Users can belong to several Spaces. The creation, change and deactivation of user accounts are logged.

Can AllocNow staff access customer data?

AllocNow staff have no standing access to customer application data. Access is limited to a small number of named operations staff using personal accounts with MFA. It is granted only on a need-to-know basis, for example for support or incident handling, and is bound by the confidentiality obligations in our Terms & Conditions and Data Processing Agreement.

How does AllocNow control its own employees' access?

Every employee has a personal account with mandatory multi-factor authentication; administrators use phishing-resistant MFA. Access follows least-privilege principles, privileged access is time-limited and logged, and access is reviewed annually and revoked on departure.

Data protection and privacy

Is PharmaLCA compliant with the GDPR?

Yes. AllocNow processes personal data in accordance with the GDPR and the German Federal Data Protection Act (BDSG), and has appointed a Data Protection Officer. Both plans are covered by the PharmaLCA Terms & Conditions, which include a Data Processing Agreement (Annex A).

Which personal data does PharmaLCA process?

Personal data is limited to user account data:

- Account data: email address, first name, last name and MFA information, kept until the account is deleted.
- Session data: a session ID cookie in the browser and tokens stored server-side.
- Logs: sign-in and application logs, retained for up to one year.

The LCA models, datasets and results entered by users are business data of the customer.

Does PharmaLCA use artificial intelligence?

No. PharmaLCA currently contains no AI functionality, and no customer data is sent to AI services.

Is customer data used for other purposes, such as AI training?

On the Professional plan, no. Customer data is stored and processed only for the customer's own assessments and is never used for AI training, analytics or any other secondary purpose. On the Starter plan, AllocNow may use customer data for other purposes as set out in the PharmaLCA Terms & Conditions. This does not include personal data.

Which sub-processors are involved?

Sub-processor	Purpose	Data involved
Amazon Web Services EMEA SARL	Hosting, compute, storage, user authentication and system emails (Frankfurt, Germany)	All application data; account and MFA data
Cloudflare, Inc.	Bot and abuse protection on sign-in and registration forms (Turnstile)	Challenge token; IP address and browser signals of the user solving the challenge

Before engagement, AllocNow assesses critical suppliers, such as cloud and hosting providers, for their security certifications (for example ISO/IEC 27001 or SOC 2), hosting region and contractual compliance.

How long is data retained, and how is it deleted?

- Customers may request deletion at any time.
- On request, or at the end of the retention period, data is deleted from production systems using secure deletion methods.
- Backup snapshots expire automatically after 14 days.
- Logs are deleted automatically after one year.

Secure development and vulnerability management

How is security built into software development?

AllocNow follows a documented secure development lifecycle aligned with the OWASP Top 10. All changes are peer-reviewed, automatically tested and scanned before release, and production deployments are approved and logged.

How are changes and releases managed?

Changes are deployed only through the reviewed release pipeline. Releases are versioned and communicated through release notes in the application. As PharmaLCA is a standard multi-tenant SaaS product, releases are not subject to individual customer approval.

How are vulnerabilities identified and fixed?

Dependencies are updated continuously, container images and dependencies are scanned automatically, and vulnerabilities are rated using CVSS v3 and fixed within the following time frames:

Severity (CVSS v3)	Remediation time
Critical (9.0–10.0)	Within 7 days
High (7.0–8.9)	Within 30 days
Medium (5.0–6.9)	Within 90 days

Is PharmaLCA penetration tested?

Yes. Independent penetration tests are carried out at least annually, and findings are tracked to resolution. The most recent test, a white-box penetration test and code audit by Cure53 in July 2026, covered the web application, the API and the underlying infrastructure.

Business continuity, backup and incident management

How is data backed up?

The PharmaLCA databases are backed up automatically every day. Backups are encrypted, stored redundantly and retained for 14 days. AllocNow's ISMS requires restore tests at least once a year.

What are the recovery objectives?

Objective	Value
Recovery time objective (RTO)	8 hours
Recovery point objective (RPO)	24 hours

Business continuity and disaster recovery plans are documented under the ISO/IEC 27001 ISMS, and the infrastructure can be rebuilt from code.

How are the platform and security events monitored?

Platform health and security events are monitored continuously, with alerts routed to the responsible staff. Sign-in and application logs are retained for up to one year.

Does PharmaLCA keep an audit trail of data changes?

PharmaLCA is not a GxP system, and personal data is limited to user account data. The creation, change and deactivation of user accounts are logged, but a full audit trail of every read, write and delete operation on application data is not available.

How are security incidents handled?

- AllocNow operates a formal, documented incident management process with defined roles, including a Data Breach Policy, under its ISO/IEC 27001 ISMS.
- Incidents are reported to information-security@allocnow.com, then classified and evaluated by the Information Security Officer. High-severity incidents are escalated to management.
- Customers are notified of personal data breaches without undue delay, and at the latest within 72 hours, as set out in the Data Processing Agreement.
- Each incident is followed by a review of its causes and of any changes needed to systems or procedures.

Service levels and support

What availability does AllocNow commit to?

For the Professional plan, the Service Level Agreement (Annex B to the PharmaLCA Terms & Conditions) commits to 99.5% monthly uptime, excluding scheduled maintenance, with service credits of 5–15% if this is not met.

When does maintenance take place?

Where possible, scheduled maintenance takes place outside core hours (Monday to Friday, 09:00–18:00 CET) and is announced at least 48 hours in advance. Emergency maintenance may be carried out without notice.

How is support provided?

Support is provided by email at support@allocnow.com, Monday to Friday, 09:00–18:00 CET. Users are also supported by user documentation and tutorial videos. AllocNow operates the service itself; no system integrator is involved.

Which contractual documents apply?

Both plans are provided under the PharmaLCA Terms & Conditions, including the Data Processing Agreement (Annex A). For the Professional plan, the Service Level Agreement (Annex B) also applies, and the subscription is concluded via an Order Form. PharmaLCA is a standard product; customer-specific developments are not part of the service.

Contact for security inquiries

For further questions, completed questionnaires or supporting evidence such as the ISO/IEC 27001 certificate, please contact us:

Topic	Contact
Information security and incident reporting	information-security@allocnow.com
Data protection	privacy@allocnow.com
Product support	support@allocnow.com

AllocNow GmbH, Friedrich-Ebert-Strasse 17, 53177 Bonn, Germany · www.pharmalca.com