CovaSyn

SIG Lite (CovaSyn edition)

As of: 2026-08-04

Pre-filled answers across the topic areas of a SIG Lite questionnaire. Every answer describes the actual situation. Where something is not in place, the answer says so along with what compensates for it.

This edition is generated from a single maintained answer library. One edit takes effect in every edition at once. Statements describe the actual situation; where something is not in place, the answer says so explicitly.

SIG A · Risk and security governance

Is a documented information security management system in place?

Status: Partial

Security policies, the access concept, the deletion concept and the incident response plan are documented and reviewed annually. There is no ISO 27001 certification; it is in preparation with a documented statement of applicability. CovaSyn is a small company and responsibility sits with named management.

Evidence: Trust page, compliance posture section

Do you hold certifications (ISO 27001, SOC 2, TISAX)?

Status: No

No. ISO 27001 is in preparation, SOC 2 is not planned, TISAX is not relevant for our market. We do not claim certifications we do not hold. We will pursue certification as soon as a concrete customer contract requires and funds it.

Is there a change notification policy for model and tool changes?

Status: Yes

Yes. Tool versions are pinned, identical input reproducibly yields identical output. Changes to numerical tools or to a language model in use that can affect results are announced at least 30 days before they take effect, naming the affected tool and the expected impact. For validated customer processes this is the basis of your change control.

Evidence: Changelog on covasyn.com, enterprise framework agreement

SIG D · Access control

Is single sign-on supported?

Status: Yes

Yes, SAML 2.0 for enterprise customers, proven with Microsoft Entra ID, Okta and Google Workspace. On first login, users are automatically assigned to the organisation based on the verified company domain. SCIM for automatic deprovisioning is available on request.

Evidence: SSO setup guide for your IT

How is administrative access to production systems governed?

Status: Partial

Administrative access to the application environment is exclusively over SSH with registered key pairs; password login is disabled for the administrative account. There is no shared generic account and no further login accounts on the system. Stated openly: exactly one key is currently registered, a second named access is being set up. Access to customer data happens only for a concrete incident, and logins are logged by the system.

Are accesses logged and are the logs exportable?

Status: Yes

Yes. Every tool call is logged with timestamp, tool, version, outcome and key identifier. Logs are exportable as CSV or JSON. Outputs carry a SHA-256 hash, so post-hoc modification of a log entry surfaces on re-hashing.

SIG G · Operations, network and encryption

Where is data hosted?

Status: Yes

In Germany, at Hetzner Online GmbH. Data is held within the EU, with no mirroring outside the EU. On request, deployment as a container on your own infrastructure is possible.

Is transport encrypted, and how is data protected at rest?

Status: Yes

Transport runs exclusively over TLS 1.2 or higher, with HSTS enabled. At rest, storage volumes are encrypted; credentials and keys are held as hashes or in separate configuration and are never logged in clear text.

Are security updates and dependencies checked regularly?

Status: Yes

Yes. Every code revision automatically runs type checking, tests, a dependency audit and a scan for accidentally committed secrets. A red run blocks the release.

SIG I · Incident management

How are security incidents handled and reported?

Status: Yes

A documented reporting path with named responsibilities is in place. Affected customers are informed without delay, at the latest within 24 hours of identifying an incident that may relate to their data. The Art. 33 GDPR notification deadline towards the supervisory authority (72 hours) is part of the procedure. External security reports are accepted at security@covasyn.com.

Evidence: security.txt per RFC 9116, security page

Are availability and errors monitored?

Status: Yes

Yes, with self-hosted availability monitoring and error tracking, alerting by email. Error tracking is deliberately built so that it captures no request bodies, no query parameters and no uploaded content. We only state a committed availability figure once it has been measured over 30 days; a proven number is worth more than a promised one.

SIG K · Business continuity

How are backups and restoration handled?

Status: Partial

The database is backed up automatically every day at 03:00 UTC with a retention of 7 days. A snapshot is also taken before every deployment. Targets: recovery time under 8 hours, maximum data loss 24 hours. Stated openly: backups currently reside encrypted on the same host system as production; an off-site copy and a regularly documented restore test are being implemented. For enterprise customers we agree different retention periods and separate storage contractually.

What happens if the provider fails or ceases to operate?

Status: Partial

CovaSyn is a small company and we say so openly. Two people hold full administrative access, an operations manual exists, and your data is fully exportable at any time. For enterprise customers, running on your own infrastructure is the most robust safeguard; the material required for that is part of the contract.

SIG P · Privacy

Is customer data used to train models?

Status: No

No. Uploaded structures, sequences and files are processed solely to answer the respective request and are never used to train our own or third-party models. This commitment is contractual in the data processing agreement, not just website copy. Contracts with the model providers we use exclude training on transmitted data.

Evidence: DPA, purpose limitation clause, trust page

How is tenant separation implemented?

Status: Yes

Every record belongs to an account, and separation is enforced at row level in the database (row level security), not only in the application. Access through a foreign account returns no rows, not a filtered view. Enterprise customers can additionally run single-tenant or on their own infrastructure.

Evidence: Trust page, technical description on request

Is data deleted on request, and what are the retention periods?

Status: Yes

Yes. On request we delete customer data within 30 days, including backup copies within their rotation cycle (7 days at most). After contract end, processing data is deleted within 90 days. Invoice records subject to statutory retention (10 years under German commercial and tax law) are excluded and contain no analysis content.

Evidence: Deletion concept, DPA

Is personal data transferred to third countries?

Status: Partial

Yes, in part. The computational tools themselves run on our infrastructure in the EU. Two functions do however involve a language model from Anthropic with processing in the United States, and content is transmitted in the process: the chat assistant in the structure editor (transmits the drawn structure, the conversation history and the results of the tools invoked) and the interpretation feature in the campaign analysis area (transmits result summaries and statistical evaluations, no raw structures). The transfer is covered by standard contractual clauses and Anthropic is listed in the subprocessor list. All other tools, including retrosynthesis, spectra prediction and toxicology, operate without a language model and without third country transfer. Enterprise customers can run the platform entirely on their own infrastructure, in which case no transfer takes place at all.

Evidence: Subprocessor list, DPA annex, architecture description on request

Who owns the rights to uploaded content and results?

Status: Yes

Rights to your inputs and to the generated results remain entirely yours. CovaSyn acquires no usage rights beyond delivering the service. This is expressly governed in the framework agreement.

Evidence: Enterprise framework agreement, rights section

SIG U · Artificial intelligence

Are results deterministic or probabilistic?

Status: Yes

The numerical tools are deterministic: pinned versions, identical input reproducibly yields identical output, also weeks later. A language model may sit in front to understand the task, never inside the computation. That separation is why the results are auditable.

Which model providers are used and what happens to data there?

Status: Yes

We use a language model from Anthropic (Claude) at exactly two points, both clearly delimited: the chat assistant in the structure editor and the interpretation feature in campaign analysis. What is transmitted there is the structure being worked on, the conversation history and results of the tools invoked, respectively statistical evaluations. Processing takes place in the United States, covered by standard contractual clauses; under the provider's commercial terms no training takes place on transmitted content. All other tools, meaning retrosynthesis, spectra prediction, toxicology, stability and chromatography, use our own models specialised for chemical tasks on our infrastructure in the EU and transmit nothing to third parties. You can recognise the two exceptions by the fact that they are dialogue-based features rather than computational tools. Changes to the provider list are announced with a right to object.

Evidence: Subprocessor list

SIG V · Regulatory and contractual

How is the software categorised under GAMP 5, and do you deliver a validated system?

Status: Partial

The categorisation is GAMP 5 category 4 (configured product); no bespoke code is developed at the customer site. We do not deliver a validated system, we deliver the material with which you validate: templates for user requirement specification, functional specification and installation, operational and performance qualification. Validation is a process in your organisation, not a property software carries at purchase. That is the normal case in pharma.

Evidence: Validation pack in the enterprise tier

Do you offer a data processing agreement under Art. 28 GDPR?

Status: Yes

Yes, including the annex on technical and organisational measures under Art. 32 GDPR and the subprocessor list. The agreement is made available on request before the pricing conversation.

Evidence: DPA on request