

# Third-Party Services Policy

## I. Purpose

Nested Knowledge's products offers a web-based software-as-a-service application and customer support services, including notices of new releases. This policy ensures that third party services used by Nested Knowledge undergo appropriate risk and data protection assessment.

## II. Scope

## III. Third-Party Service Policy

A list of sub-processors and third-party service providers is maintained below. The list is updated at least annually.

### Monitoring for Vulnerabilities

Developers monitory third party providers for breaches and vulnerabilities, and notify the Technical Lead by email or slack when a breach is detected.

If a security breach is detected, we:

- Evaluate the severity of the incident and determine the urgency of response and resource deployment.
- Identify the classes of data affected by the breach.
- Remove the service provider, or modify use of the service provider.
- Disclose the security incident to users.
- If applicable, we escalate to clients by following the chain on communication described in our service license agreement.

Third party processors are similarly monitored for policy changes, specifically with regard to changes impacting [regulatory requirements](#).

### Summary of Sub-processors

Subprocessors handle user data processing tasks on behalf of the software application.

Name (Manufacturer)	Data Processing Agreement	Critical to application?	Purpose	Data Processed
Airplane.dev	Signed, available upon request <a href="https://airplane.dev">https://airplane.dev</a>	No	Internal customer support applications	User emails and billing data

Name (Manufacturer)	Data Processing Agreement	Critical to application?	Purpose	Data Processed
Auth0	<a href="#">Auth0 DPA</a>	Yes	Authentication of user accounts	User emails & credentials
HubSpot	<a href="https://legal.hubspot.com/dpa">https://legal.hubspot.com/dpa</a>	No	Send release and marketing emails to users	User emails
Metabase	<a href="https://www.metabase.com/license/hosting">https://www.metabase.com/license/hosting</a>	No	User analytics	User accounts & activity
OpenAI	Signed, available upon request	No	Screening model features	Record abstracts
Scite	<a href="https://scite.ai/policy">https://scite.ai/policy</a>	No	Screening model features, record display badge	Record DOIs
Stripe	<a href="https://stripe.com/legal/dpa">https://stripe.com/legal/dpa</a>	No	Payment services	User email, location, subscription, and payment details

## List of Infrastructure Providers

Infrastructure Providers house the physical hardware used to run the application. These providers do not process user data, although they contain it.

Name (Manufacturer)	Data Processing Agreement	Purpose
AWS (Amazon)	<a href="https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html">https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html</a>	Production Infrastructure (servers, services, databases)
GCP (Alphabet)	<a href="https://cloud.google.com/terms/data-processing-addendum">https://cloud.google.com/terms/data-processing-addendum</a>	Storage of production database backups

## List of third-party providers

Third-party provider offers services that are integrated into the application in an opt-in manner or without processing user data, and are not necessary for core functionality.

Name (Manufacturer)	Data Processing Agreement	Critical to application?	Purpose	Data Processed
EuropePMC		No	Run searches against EuropePMC	Literature Searches

Name (Manufacturer)	Data Processing Agreement	Critical to application?	Purpose	Data Processed
DOAJ		No	Run searches against DOAJ	Literature Searches
Plausible		No	Web and Mobile analytics	Page visit URL
Pubmed Entrez API		No	Run searches against PubMed	Literature Searches
Unpaywall		No	Full text retrieval	Record DOI
<a href="#">ClinicalTrials.gov</a>		No	Run searches against ClinicalTrials.gov	Literature Searches

## IV. Third-Party Services and Data Protection

The [Policy Privacy](#) describes the data Nested Knowledge shares with third party service providers.

### Contracts with Third Parties

Contracts with third party service providers must incorporate information security requirements, including data protection and notices of security incidents.

We will document roles, responsibilities, and controls between Nested Knowledge and third parties, where applicable. Documentation and risk assessment should be stored in our filesystem drive in the respective directory for the third party provider.

### Compliance and Updates

At least annually, we will review third parties vendors to assess compliance with contracts and security standards, and we update the privacy policy accordingly.

### Communicating Updates

When new third party vendors are to be added, data supplied to vendors is to change, or the vendor's processing agreement are to change, all users will be notified via email with at least 7 days notice.

## Revision History

Author	Date of Revision/Review	Comments/Description
K. Kallmes	1/26/2023	Reviewed
K. Cowie	1/26/2023	Drafted
K. Holub	9/28/2023	Monitoring updates

[Return to Policies](#)

Last update:  
2023/09/29 02:22

wiki:policies:third\_party [https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:third\\_party&rev=1695954168](https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:third_party&rev=1695954168)

---

From:  
<https://wiki.nested-knowledge.com/> - **Nested Knowledge**

Permanent link:  
[https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:third\\_party&rev=1695954168](https://wiki.nested-knowledge.com/doku.php?id=wiki:policies:third_party&rev=1695954168)

Last update: **2023/09/29 02:22**