Third-Party Services and Subprocesors 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-processsors 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 https://airplane.dev	No	Internal customer support applications	User emails and billing data

Name (Manufacturer)	Data Processing Agreement	Critical to application?	Purpose	Data Processed
Auth0	Auth0 DPA	Yes	authentication of users accounts for the NK application.	User email and password or social login account identifiers and Login history
HubSpot	https://legal.hubspot.com/dpa	No	Send release and marketing emails to users	Full name and email addresses of users. Users can have their personal or organizational data deleted at any time. All user data is deleted from HubSpot if an account is deleted.
Metabase	https://www.metabase.com/license/hosting	No	User analytics	User accounts & activity
OpenAI	Signed, available upon request	No	Screening model features	Record abstracts
Scite	https://scite.ai/policy	No	Screening model features, record display badge	Record DOIs
Stripe	https://stripe.com/legal/dpa	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	Data Processed
AWS (Amazon)	https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html	Production Infrastructure (servers, services, databases)	All user accounts and data generated on the NK application are stored in databases in AWS, behind a firewall (VPC). This data, including personal information, is not shared with AWS in a structured or meaningful way, instead only being processed by NK application code within the VPC.
GCP (Alphabet)	https://cloud.google.com/terms/data-processing-addendum	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
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
ClinicalTrials.gov		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 subprocessors are to be added, data supplied to vendors is to change, or the vendor's processing agreement are to change, all affected users will be notified via email with at least 7 days notice.

V. Third-Party Provider Data Breaches

Timestamp	Event	Description	Reporting	Status
03-20-2023 1:00AM PT - 10:00 AM PT			Open AI Statement	
03-18-2023	Compromised employee account	Affected 30 accounts in the Cryptocurrent industry	Hubspot statement	No impact on Nested Knowledge data.

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