Lexis+ AI Security Information

LexisNexis® prioritizes security in everything we do. Our products are built with a development philosophy that prioritizes customer data protection from the ground up.

Our comprehensive data protection program ensures that we safeguard your valuable information. To ensure comprehensive security controls throughout the entire product lifecycle, we've assembled a team of application and security experts. They work hand in hand with our talented product development and operations teams, ensuring that each product meets rigorous, audited standards.

Security, Privacy and Trust: Our Promise

Experience unrivaled security and cutting-edge technology with LexisNexis® solutions. Trust us to protect your valuable assets while delivering top-notch performance.

Please use the navigation links below to brief yourself about our commitments to your data.

DATA	ENCRYPTION	AUDITS & POLICIES	SECURITY & ACCESS CONTROL
ARCHITECTURE	Q & A	CONTACT	OTHER MATERIALS

DATA

Your Prompts

- Your conversations are **purged after 90 days or until the user deletes** (whichever occurs first)
- Your conversation history is stored in a **secured** environment and **encrypted-at-rest** using **AES-256**
- LexisNexis Large Language Model partners are bound by our agreement to **not train** our custom models based on your data.
- Our Cloud providers have logging for support and troubleshooting purposes and have *no access to user prompts*.

Your uploaded Documents

- Your documents are under your control. Documents can be removed by deleting the session conversation thread or our system will **purge** them after a **10-minute inactivity**.
- Your documents are retained for the duration of an **active, in-progress session**.
- Your conversations related to the documents uploaded are **purged after 90 days or until the user deletes** (whichever occurs first)

Privacy by Design principles are integrated into the development process with a compliance oversight to ensure LexisNexis® solutions **comply** with all applicable **privacy and data protection laws**. All staff are required to undergo data protection training as part of company training procedures. This is supplemented with regular and annual compulsory compliance training on data protection and data security. LexisNexis has data protection and confidentiality clauses in employment/service contracts.

ENCRYPTION

All Lexis+ AI™ customer data (prompts/documents) is encrypted at rest, utilizing AWS's Key Management Service and **AES-256** encryption. Internet traffic in transit using TLS 1.2. Each customer request is treated separately and subsequently generates a separate transaction with the generative capabilities.

AUDITS & POLICIES

LexisNexis engages an independent third-party auditor to perform an annual **SOC 2 Type 2** examination of Lexis® and Lexis+ based upon the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality and Privacy. New assets for Lexis+ AI have a SOC2 examination scheduled for Q1 2024.

LexisNexis has a **robust** set of Information Security policies. This enables us to efficiently respond to **potential threats** against our systems. Our incident response plans, which are **updated and tested periodically**, include technical, administrative, business, and executive escalation processes. The company does have external firms on retainer to provide expertise and guidance, as needed.

SECURITY & ACCESS CONTROL

Network security controls are implemented based on a least access principle. The controls also provide protection against unauthorized access and traffic interception. These protections are in place to restrict access inbound and outbound along with internal traffic to/from systems. Where possible and necessary, private endpoints are utilized to securely access cloud services to ensure security of associated transactions.

Access to company networks is restricted to corporate managed devices and uses multi-factor authentication. Authorizations are based on least privilege principle. Privileged accounts are provided based on need to perform job function and approved by management, with regular access reviews undertaken. Access is automatically removed upon termination.

The LexisNexis® Vendor Management program performs vendor **security and background checks and assessments** during the procurement process. Vendors are assessed on a risk-based approach using several factors including access to data (customer/company), system access, and performing a critical function on behalf of the company.

We conduct penetration testing with internal tools and third-party firms to validate our defenses. Automated internal and external vulnerability scanning provides continuous visibility into new risks. Any items discovered are tracked centrally to ensure proper risk prioritization. Remediation efforts are coordinated with the supporting team in risk prioritized manner.

ARCHITECTURE

Lexis+ AI will be deployed and maintained using the same security architecture, reviews, audits, and validation as Lexis+® and our other products. Generative AI capabilities have been engineered and deployed to meet our high-level security standards, with a key focus on protecting and segmenting customer activity. Our security team continues to be actively engaged in all aspects of the engineering and deployment of Lexis+ AI.

High-level architecture flow:

1. A user's prompt/ask/document is sent securely using **TLS 1.2** to Lexis+ servers.

2. The prompt is parsed for intent and broken down into separate queries by an embeddings model to retrieve information from our content store.

3. The prompt, along with content response, is then sent using **TLS 1.2** to our private Large Language Model hosted within **AWS Bedrock (Claude2)/Azure (OpenAI GPT4)**

4. A grounded, generated response is then presented to the user in Lexis+ AI.

5. User prompts and responses are retained for up to 90 days as part of their conversation history in a secured and encrypted database (**AES-256**). Documents are **purged** after a **10-minute session inactivity.**

6. Anthropic and OpenAI do not have access to our models or service. Our architecture **precludes either organization from logging or training models** based on users' conversations.

7. AWS Bedrock and Microsoft Azure Cloud services both have logging for **support and troubleshooting purposes** and has no access to users' prompts.

Q & A

Will my entries into the tool be used to train the Lexis+ AI model?

LexisNexis does not use customer data to train our Large Language Models. Users also have individual control of prompt history and options to delete prompt history from our services. For further information, you can access our privacy policy at https://www.lexisnexis.com/en-us/terms/privacy-policy.page

Will Lexis+ AI utilize third party systems to process my data?

LexisNexis utilizes third-party providers of AI technology to ensure our AI solutions leverage the best in new generative AI capabilities. All third-party providers of AI technology have been vetted through our security review processes.

Third-party models used in Lexis+ AI are deployed only in **protected, private cloud** environments in AWS Bedrock and Microsoft Azure that are part of the secure LexisNexis cloud environment and subject to LexisNexis security controls that apply across our platform. The models are used exclusively by LexisNexis and **not used by the public** or other companies.

All models deployed by LexisNexis utilize dedicated, encrypted, authenticated connections which meet or exceed our high security standards. All data is encrypted and stays in the control of LexisNexis at all times.

What are your encryption standards?

All Lexis+ AI customer data (prompts/documents) is encrypted at rest (**AES-256**) and traffic in transit (**TLS 1.2**).

Can LexisNexis employees see my chat queries?

A restricted group of product support experts with appropriate accesses will be able to review customer usage data for the purpose of product support and technical troubleshooting. Access is limited only to authorized personnel and customer association is pseudonymized.

What about my uploaded documents – do you retain them?

Uploaded documents are securely stored in a temporary AWS cache for the duration of your session. All documents are purged after 10 minutes of inactivity, or a user can purge a document by deleting the session conversation thread.

Can firm administrators limit use of Lexis+ AI to certain features or users within the firm?

Yes, firm administrators are able to limit individual user access to Lexis+ AI at the firm.   Administrators will also have the option to temporarily disable the Document Upload and Drafting tasks for their enterprise in the event of any outstanding information security questions or concerns.

Where can I find documents and reports related to your audits and policies?

All reports and documents are available on a per-request basis. Contact your account team for more information.

Is my Lexis+ AI data made available to other Lexis services within LexisNexis?

Customer data is only be made available in the product context in which it has been entered, and not shared with other products unless explicitly granted and communicated.

CONTACT

security@lexisnexis.com

privacy.inquiries@lexisnexis.com

OTHER MATERIALS

LexisNexis Legal & Professional Data Privacy Principles

Responsible Artificial Intelligence Principles at RELX

Your Peace of Mind Is Our Priority

In-depth InfoSec Document - Available Upon Request

Detailed Architectural Drawings - Available Upon Request

Learn more **LexisNexis.com/AI**