



☰ Security and Privacy > Data processing and privacy

Security and Privacy

Data processing and privacy

📄 Copy page



Default query processing regions, GDPR scope for customer data, ZDR, and enterprise processing controls.

This page describes how Linkup handles customer data and query processing, including default behavior and configurable options.

Contact and key links

- Privacy requests: privacy@linkup.so
- Configurable processing options: contact@linkup.so

Sign a DPA



Execute a Data Processing Agreement via DocuSign.

Request Zero Data Retention



Book a call to scope and enable ZDR.

Customer data

Linkup is GDPR compliant for customer data. A Data Protection Officer oversees compliance with the EU's General Data Protection Regulation (GDPR), the ePrivacy Directive, the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), and other applicable data protection laws. GDPR is the baseline standard for customer data protection.

Data Processing Agreements (DPAs) aligned with GDPR Article 28 are available on request and can be signed via DocuSign.

Query processing

Linkup operates infrastructure in the US, EU, Canada, and APAC.

By default:

- Queries may be processed across these regions based on load allocation
- Local query processing is not guaranteed

Under enterprise agreements, Linkup can configure:

- Guaranteed local query processing in a specified geography
- Multi-routing so that queries from different regions are processed locally according to regional requirements

Zero Data Retention (ZDR)

ZDR can be requested on demand. It is not enabled by default.

Zero Data Retention ensures search queries and results are never written to persistent storage.

When ZDR is enabled:

- **No query logging:** Search queries are not logged or stored on Linkup systems
- **No result retention:** Results are not retained after delivery to the client

How it works

Linkup can offer ZDR because its retrieval is built on its own search index and processing stack. Queries are handled on infrastructure Linkup operates and controls.

ZDR requests are processed in temporary computing environments where data is held only in memory (RAM) during processing. No data is written to persistent storage. Once results are returned, temporary data is destroyed and cannot be recovered.

When to use ZDR

ZDR is typically requested by organizations in regulated industries or those handling sensitive competitive intelligence, where even temporary storage raises compliance or confidentiality concerns.

To request ZDR, [book a call](#) or contact `contact@linkup.so`.

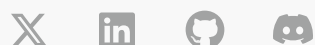
For a detailed explanation of how ZDR works and why it matters for AI teams, see: [What is Zero Data Retention and why does it matter for AI teams?](#)

Documentation

- Trust Center: <https://trust.linkup.so/>
- Privacy Policy: <https://www.linkup.so/privacy-policy>
- DPA: [Sign via DocuSign](#)
- Terms and Conditions: [View here](#)

[← Overview](#)

[Security and compliance →](#)



Powered by **mintlify**