LinkedIn ATS Integrations

Data Security

Frequently Asked Questions

LinkedIn

In this Data Security FAQ, we'll help you understand:

How your data is shared and protected with LinkedIn

How your data is being protected through encryption, disposal, and beyond

Where to find additional resources to answer your data privacy questions

Table of contents

Data Security FAQs

Why does LinkedIn need to process data between LinkedIn and my ATS to make the integration work?

LinkedIn synchronizes data between your ATS and LinkedIn to streamline your workflow so you don't waste time switching between different platforms. The data is processed with security measures in place and in compliance with customers' instructions.

Who controls my ATS data?

You are always the controller of your personal data as defined in the LinkedIn Subscription Agreement (LSA), or your governing LSA with LinkedIn

Does LinkedIn share my ATS data with other LinkedIn customers?

No.

Does LinkedIn use my data to create or modify LinkedIn profiles?

No.

How is access to my ATS data limited & kept secure?

Only LinkedIn engineers that work on our ATS middleware platform who have been granted security approval can access this data. All access to production infrastructure is via named accounts which are attributable to a unique individual.
Access to production data is limited to select few SRE's and DBA's as necessary to perform maintenance and support the platform.

This includes access to PII (Personally Identifiable Information). Member data is logically and programmatically separated in databases and applications and all access requests and approvals are logged, reviewed and approved to ensure only appropriate access is granted and is fully auditable.

Security awareness training is mandatory for all personnel. Additional security requirements, controls, and training are in place for personnel with access to Scoped Data that includes PII. All access is logged and reviewed.

Learn more about LinkedIn's Customer Data Processing agreement and how LinkedIn is committed to keeping your data safe.

Data Security FAQs

What type of data is shared between LinkedIn and your ATS?

Candidate identity data is used to match candidates or prospects in LinkedIn Recruiter with existing candidates in your ATS.

Jobs data allows recruiters to easily link candidates they're considering in LinkedIn Recruiter to their ATS, matching them with the correct job requisition in one click.

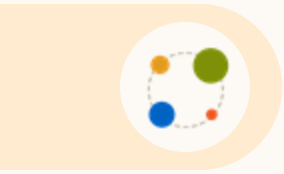
Application data will show LinkedIn members who are already in your ATS, including details about their previous application process, such as hiring outcome details and source of application.

What are minimally required fields vs optional fields?

When you activate the RSC integration, you elect from within your ATS to send all minimally required fields for RSC to function.

We recommend that you also include optional fields to optimize functionality and collaboration within your team. However, you can choose to opt-out of sending optional fields such as notes, interview feedback and certain records, such as jobs, from your ATS.

Please note: you will lose RSC functionality for these specific records after doing so. For example, you will not have the ability to export LinkedIn Member stub profiles to any job records withheld from the RSC sync.



Here's what we won't do with your data

In short, we will not use your data in any way beyond improving YOUR product experience. For example:

1. We will not share your data with other companies.
2. We will not use your candidate data to improve content coverage on LinkedIn profile.

Resume data

Resume data is a pre-requisite for a customer to activate Unified Search

Why do we need resume data?

Unified Search allows you to search for candidates across LinkedIn and your ATS. For candidates that exist in your ATS but do not have a corresponding LinkedIn profile, we are not able to rank them properly in Unified Search. We utilize the resume data to fully understand their qualifications to serve you a better Unified Search experience.

How do we protect your resume data?

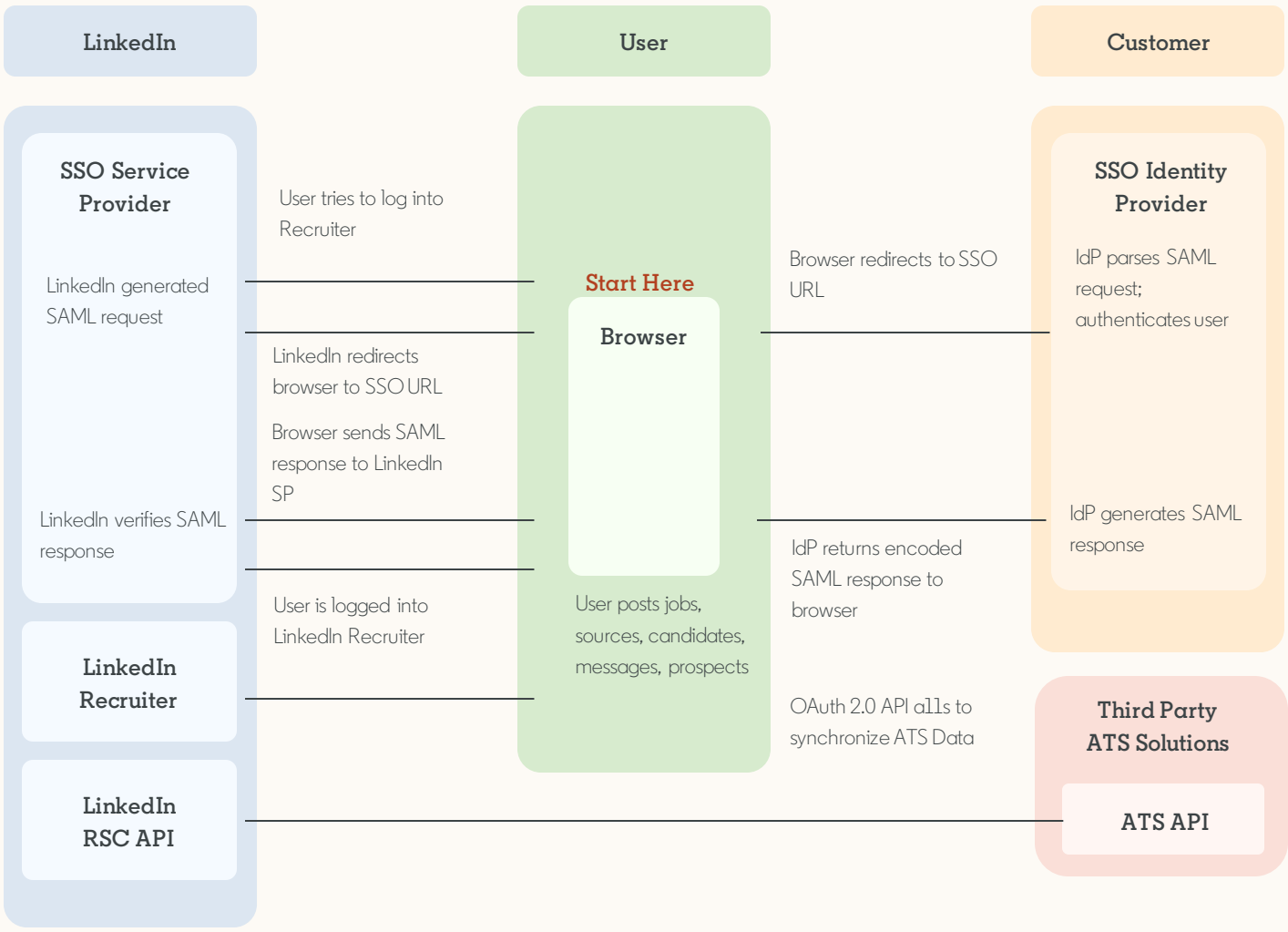
Your resume data will only be used to improve your product experience. We won't use your resume in any way beyond improving your product experience. For example, we won't use your resume data to improve other companies' Unified Search experience; we won't use your resume data to improve LinkedIn profile content coverage, etc.

LinkedIn and your ATS: Bridging your data

Our protections ensure that data flows securely between LinkedIn Recruiter, our customers, and their ATS.

LinkedIn Talent Solutions and Recruiter System Connect Data Flow Diagram

This diagram provides a high-level logical overview of the SSO login and data-flow for LinkedIn Talent Solutions and Recruiter System Connect products.



LinkedIn and your ATS: Bridging your data

How do we connect your ATS and LinkedIn data?

LinkedIn uses the Middleware Platform. It represents a common set of APIs used to: sync jobs, job applications, and talent profiles (such as candidates) between your ATS and LinkedIn on your behalf.

How are APIs authorized and protected?

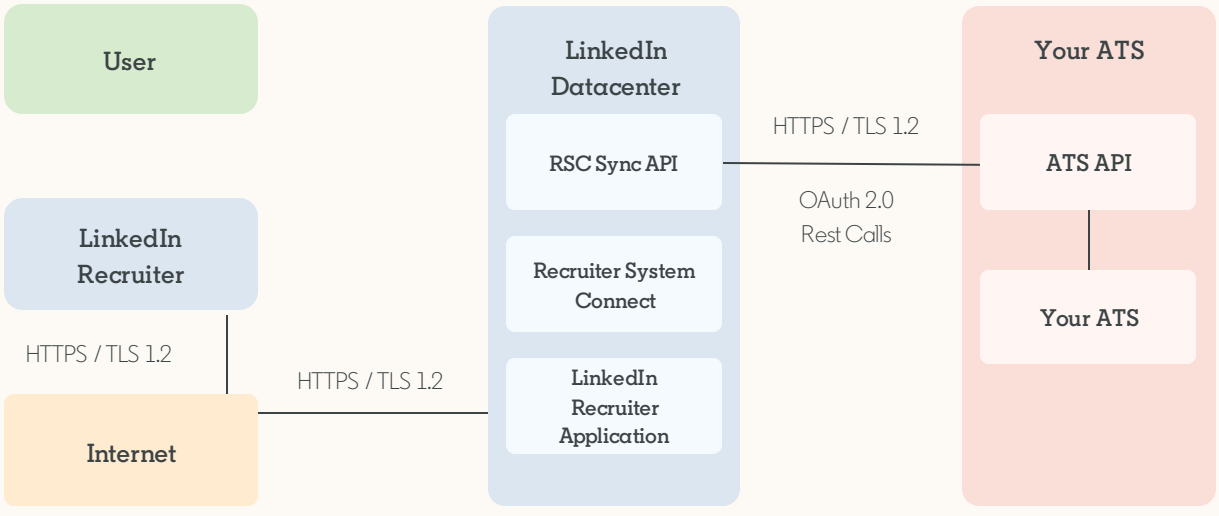
All API requests must be authorized with an OAuth 2.0 Client Credentials token. Since OAuth is used, Multi-Factor Authentication is supported on individual member accounts based on their account settings. The lowest level TLS to connect to our API is TLS 1.2; based on our SSL Report evaluating our API, we have been graded A. In addition, we use all signed certificates with URLs and APIs. We also use rate limiting on our API endpoints. For additional information on all available APIs, please visit our guide here. And, for more information on TLS requirements, see here.

Are API keys rotated?

Unless we detect abuse, we do not rotate API keys; but they can also be rotated at your request.

How are changes to products, including APIs or authentication, communicated?

If there are any changes, they will be communicated via our quarterly product release (QPR).



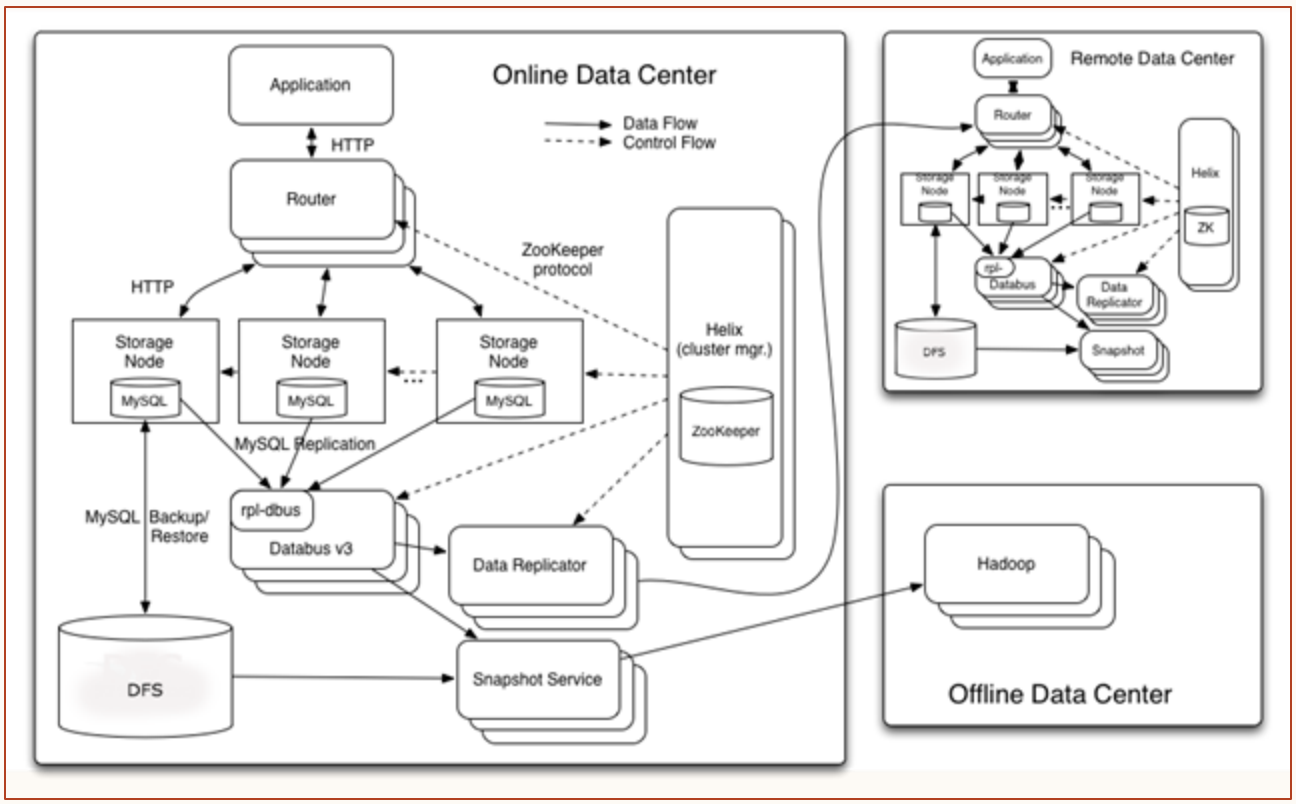
Storage, disposal & beyond

How is my data being protected through storage and disposal?

All customer data is stored in LinkedIn owned and operated data centers in the United States. Data center security, managed and controlled by LinkedIn, are the only ones that have access to these centers. LinkedIn stores this data within a Distributed Data Store. All client data is logically and programmatically segmented and secured to ensure no accidental co-mingling of client data occurs.

What database is my data stored in?

The Espresso database is our online, distributed, fault-tolerant NoSQL database that currently powers approximately 30 LinkedIn applications, including all things Recruiter. For more information on how we structure Espresso, including **data center failover, APIs, and more,** please refer to this article.



Storage, disposal & beyond

What security practices does LinkedIn use to protect my data?

LinkedIn uses password protection, data encryption, application security, physical security, and secure networks to protect customers' information residing on the LinkedIn platform. LinkedIn is SOC 2, ISO 27001, and 27018 certified - LinkedIn's ISO certifications are available for view on our Trust and Compliance site. If interested, you can request a copy of our SOC 2 report from your LinkedIn representative.

What penetration testing does LinkedIn perform?

LinkedIn performs both internal and external penetration testing. To date, we are not aware of any issues that would compromise the confidentiality and integrity of the ATS data stored on LinkedIn's platform. If you are interested in reviewing an external penetration report, ask your LinkedIn representative for a copy.

Storage, disposal & beyond

How can I disable or delete my ATS data that LinkedIn stores?
If you'd like to disable the Recruiter System Connect integration or remove this data, you can do so at any time by emailing ltsatsintegrations@linkedin.com.

If I cancel my contract with LinkedIn, what happens to my data?
Upon the termination of the data processing services , LinkedIn and any sub-processors will return all personal data and copies of such data to you or securely destroy and demonstrate them to your satisfaction. The only exception is if legal requirements prevent LinkedIn from returning or destroying all or part of the customer's data shared with LinkedIn.

What happens if a LinkedIn member deletes their account after I have exported their data into my ATS using 1-Click Export?
You will receive notice so you can make an informed decision regarding the LinkedIn member data you have exported to your ATS records, and to help ensure that you are aware of our members' choices.

If I prefer not to export candidate records from LinkedIn into my ATS, how can I turn off 1-Click Export for all users?
Navigate to your admin settings page within LinkedIn Recruiter and select off next to 1-Click Export. This setting can be updated at any time by your LinkedIn Recruiter admin.

GDPR

How can I use RSC (or ATS Integrations) in a GDPR-compliant way?

The goals of the GDPR are consistent with LinkedIn's longstanding commitment to data protection and transparency. Our integrations are built to enable customers to use it in a GDPR compliant manner. Customers are responsible for their own GDPR compliance.

Specific GDPR help center **here**

How is data encrypted by LinkedIn?

Encryption protocols, reviewed and approved by the internal LinkedIn security team, are used, where data is encrypted either at rest or in transit. A list of approved encryption protocols are maintained internally and updated as necessary based on industry standards and security research in the cryptography field.

All encryption methods used meet or exceed the standards defined by NIST Special Publication (SP) 800-175B and are currently defined as:
Minimum key length for symmetric encryption: 128 Bit AES
Minimum key length for asymmetric encryption: 2048 Bit RSA

Questions?

Below you'll find several resources to help you gain a deeper understanding of how your data is protected by LinkedIn. If you have questions not addressed by the resources below, including specific questions around access permissions, please reach out to your LinkedIn Customer Success Manager.

Where can I find additional resources to answer data privacy questions?

Where can I find additional resources to answer data privacy questions?

General LinkedIn Resources:

- LinkedIn Data Processing Agreement
- Trust and Compliance Microsite
- Privacy Policy

LinkedIn ATS Integration Resources:

LinkedIn RSC Resources:

- Microsoft Developer Documentation
- Middleware: Syncing feedback, jobs, applicants.
- Enabling RSC
- Data and Privacy for RSC: FAQs

LTSATSIntegrations@LinkedIn.com
Use this email for any technical support needs.