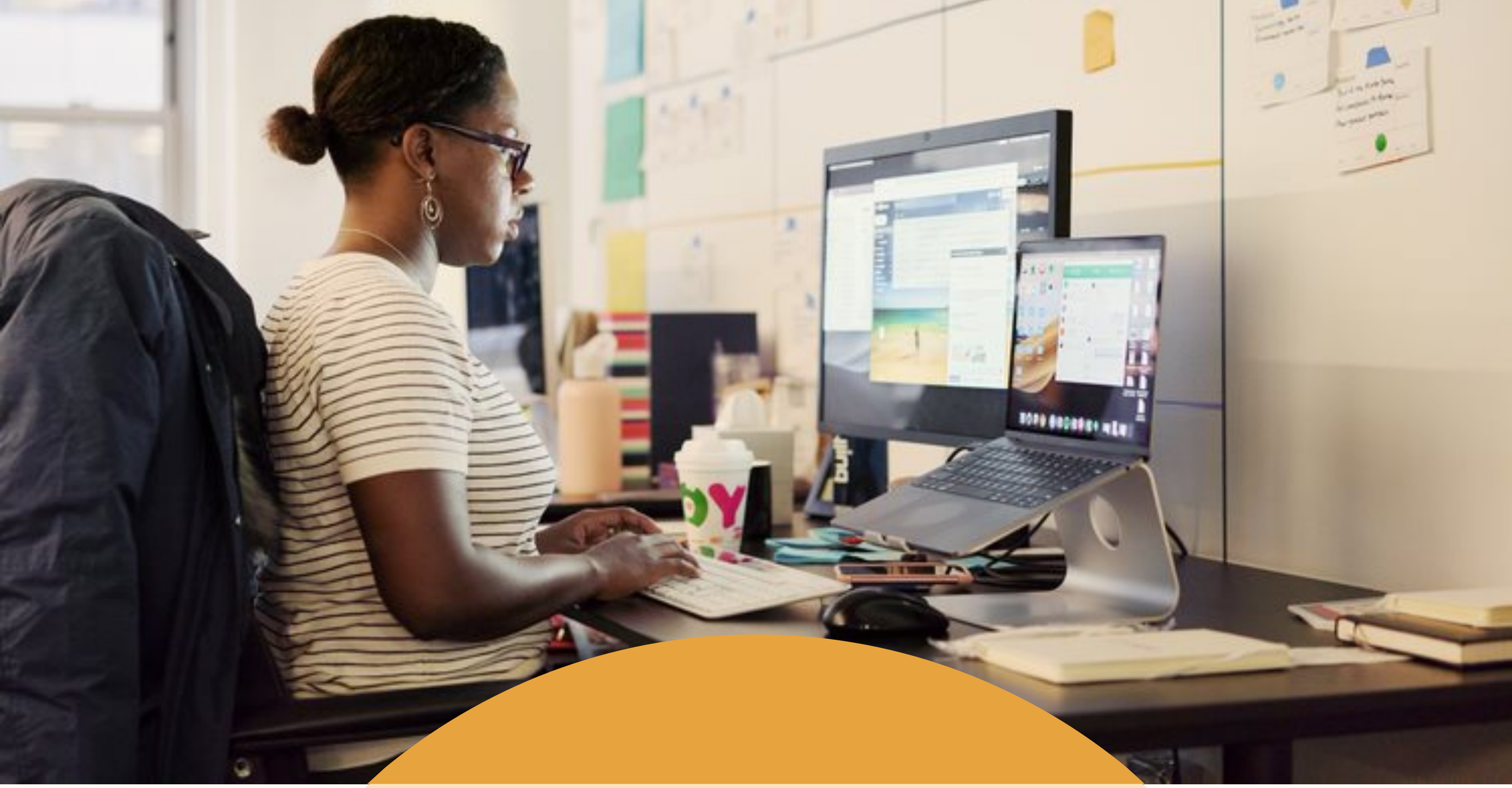


Recruiter System Connect (RSC)

Data Security

Connect LinkedIn Recruiter and your ATS with RSC to simplify the hiring process – with the confidence that your data is securely protected.

You're the boss of your ATS data

It's important to remember the golden rule: you own your ATS data. You're the boss and you're in control of your ATS candidate records.

At LinkedIn, we take pride in empowering our customers to leverage data as a competitive advantage. The benefits of integrating your ATS with LinkedIn are simple: connecting your ATS data with data living in LinkedIn Recruiter unlocks unique insights to help you create a personalized candidate experience and increase team engagement.

You're always the controller of your personal data as defined in the LinkedIn Subscription Agreement (LSA), or your governing LSA with LinkedIn. LinkedIn doesn't share your ATS data with other LinkedIn customers. We also don't use your ATS data to create or add new LinkedIn profiles or modify LinkedIn profiles with data viewable by other companies. If there ever comes a time where your team wants to end your integration with Recruiter System Connect, you can request to delete your ATS data at any time.

You're the boss of your ATS data. It's that simple.

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

- How your data is shared between LinkedIn and your ATS
- 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

Click on the titles to navigate the guide

LinkedIn and Your ATS: Bridging your data

Protecting Your Data: Storage, disposal & beyond

Resources:

LinkedIn and Your ATS: Bridging your data

We use data from your ATS to fuel efficiencies in RSC.

Once the integration between LinkedIn Recruiter and your ATS is enabled, the following data types from your ATS will be used by LinkedIn to power RSC features:

Candidate identity data - This data is used to match candidates or prospects in LinkedIn Recruiter with existing candidates in your ATS. This way you can uncover new insights about potential candidates and more effectively manage candidate pipelines. The features enabled through access to this data also help you ensure candidate information is being discovered by recruiters for the right roles.

Examples of candidate information includes first and last name of the candidate, the unique identifier of the candidate within the ATS, the candidate's email address, and the timestamp of the candidate in the ATS.

Information about Jobs - This data allows recruiters to easily link candidates they're considering in LinkedIn Recruiter to their ATS, matching them with the correct job requisition via the 1-Click job req drop down.

Application data - An In-ATS indicator in LinkedIn Recruiter 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. These candidates will also be highlighted in your Past Applicant spotlight in LinkedIn Recruiter, so you can more easily filter and prioritize candidates, who previously applied to your company and/or are in your ATS. It's important to remember any data that is owned by you is only visible to you.

Examples of application data include first and last name of the applicant, candidate email address, ATS job posting name and timestamp, application source, and the stage in which the candidate dropped off from the hiring process.

Optional Fields

If you choose to enable RSC, you must elect, from within your ATS, to send all the minimally required fields for RSC to function as designed. There are **optional fields** you can choose to opt-out of sending such as notes and interview feedback. After syncing data records for each required field, you can choose to not sync 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.

LinkedIn and Your ATS: Bridging your data

Your data stays between us.

We'll be using the data from your ATS to improve the general Recruiter experience but we won't share or display your data with any other customer. We also don't use your ATS data to create or add new LinkedIn profiles or modify LinkedIn profiles with data viewable by other companies. Additionally, if you ask us to delete your data, we'd no longer use that data to improve the general Recruiter experience.

LinkedIn processes RSC data to provide, support, and improve LinkedIn services to customers. The data is processed with security measures in place and in compliance with customers' instructions. Customers control this data while LinkedIn is the data processor.

Note: LinkedIn doesn't have plans to change how data is processed. However, planned changes will be clear and transparent.

Access to your data is limited and your data is kept secure.

Only internal employees (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.

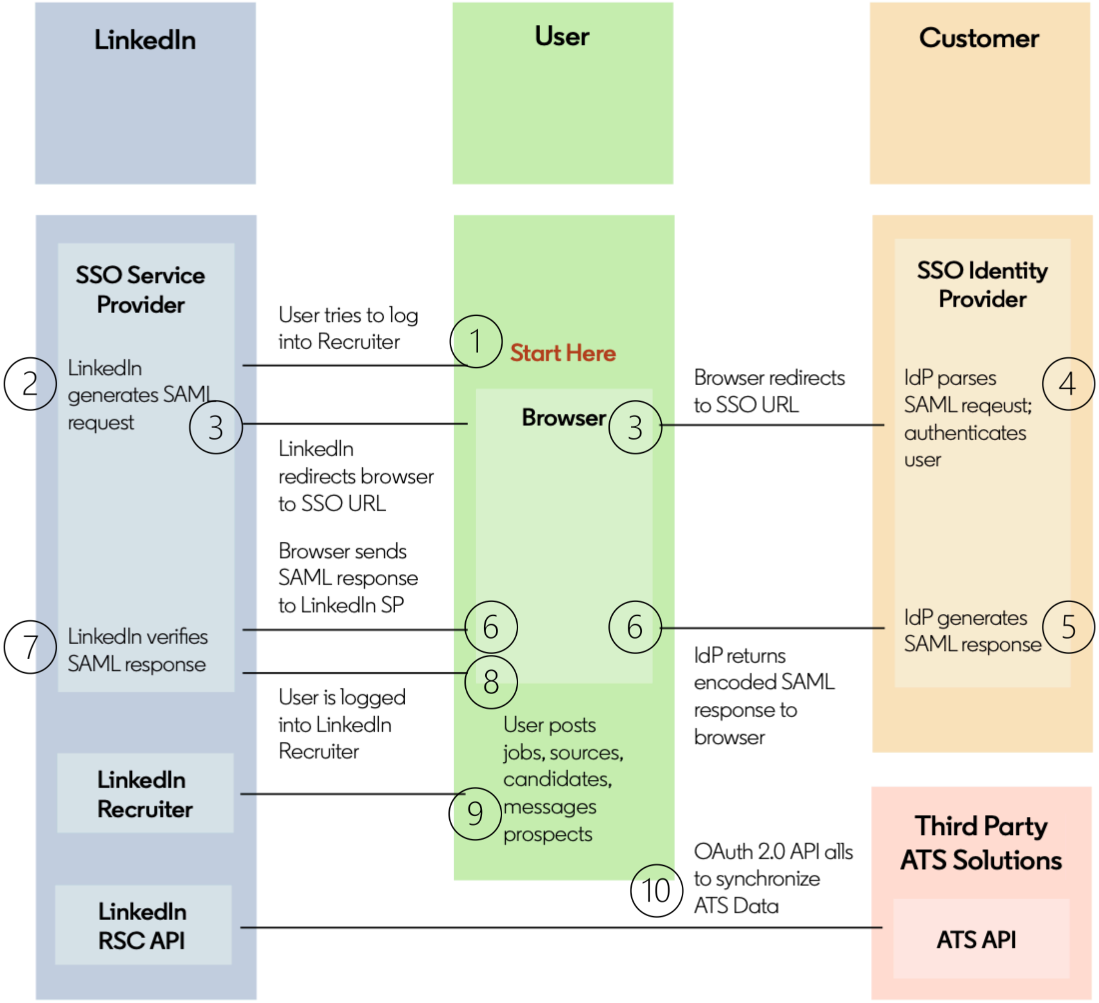
Learn more about LinkedIn's Customer Data Processing agreement and how LinkedIn is committed to keeping your data safe.

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.



User tries to log into Recruiter

LinkedIn generates SAML request

LinkedIn redirects browser to SSO URL

Browser redirects to SSO URL

IdP parses SAML reqeust; authenticates user

IdP generates SAML response

IdP returns encoded SAML response to browser

Browser sends SAML response to LinkedIn SP

LinkedIn verifies SAML response

User is logged into LinkedIn Recruiter

User posts jobs, sources, candidates, messages prospects

OAuth 2.0 API alls to synchronize ATS Data

LinkedIn and Your ATS: Bridging your data

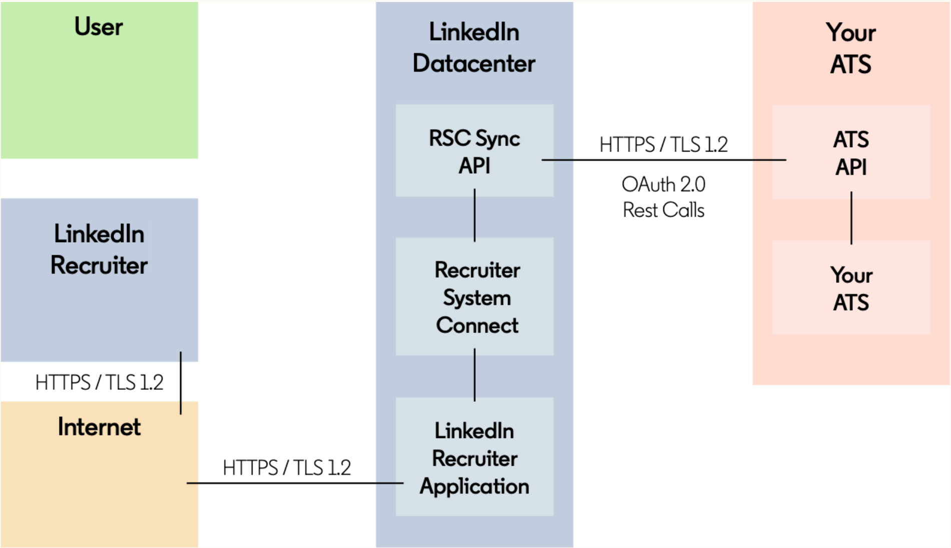
We connect your ATS and LinkedIn data with the Middleware Platform.

The Middleware Platform 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. Integrating with Middleware is essential for the Recruiter System Connect integration and powers multiple features.
All our API requests must be authorized with an OAuth 2.0 Client Credentials token.
For full information on all available APIs, please visit our guide here.

We authorize and protect our APIs.

For all data integrations, we use OAuth to make the integration process seamless and to ensure a member is always in control of their data. 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. For more information on TLS requirements, see here.

In addition, we use all signed certificates with URLs and APIs. We also use rate limiting on our API endpoints. Unless we detect abuse, we do not rotate API keys, but they can be rotated at your (the customer's) request. Reach out to your LinkedIn representative if you have questions about this request. Any changes made to our products, including APIs or authentication, will be communicated via our quarterly product release (QPR), as well as directly from your Customer Success Manager.



Protecting Your Data: Storage, disposal & beyond

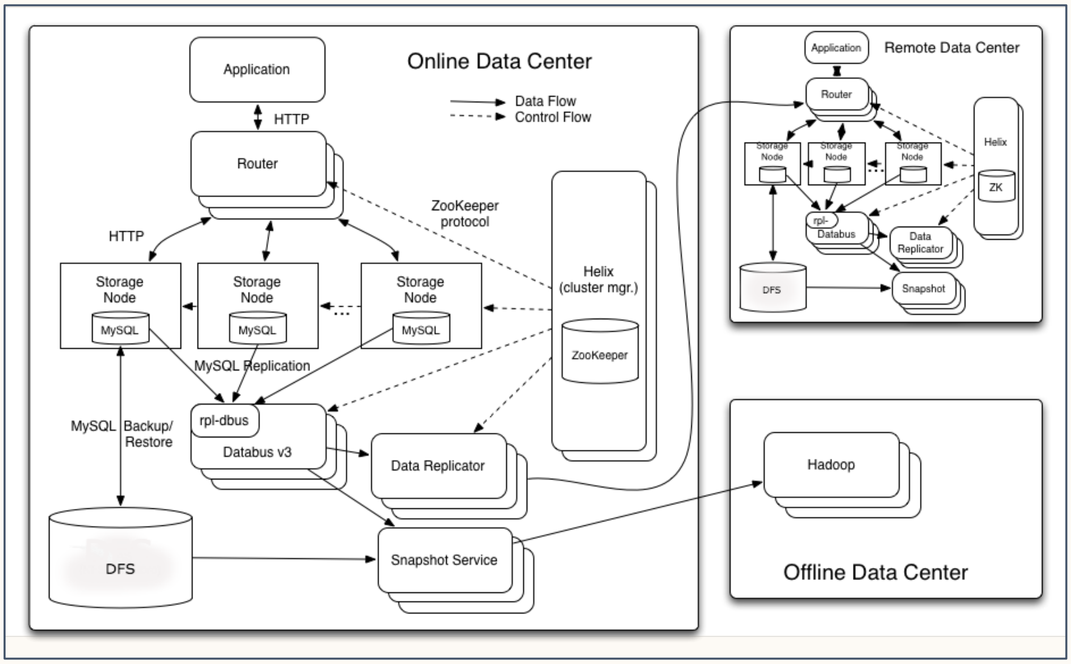
Customer data is stored and protected in our global data centers.

All customer data and personal data is stored in 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 (no caching in place). All client data is logically and programmatically segmented and secured to ensure no accidental co-mingling of client data occurs.

Data is stored in LinkedIn owned and operated data centers. LinkedIn products are multitenant and support thousands of clients. Underlying infrastructure is shared across our platform for scalability and security.

We store our data in the Espresso database.

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.



Protecting Your Data: Storage, disposal & beyond

We use industry recognized security practices to protect your 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.

For more information, or to request a copy of our SOC 2 report, please reach out to your LinkedIn representative.

We perform internal and external penetration testing.

LinkedIn performs both internal and external penetration testing, and as of date, we are not aware of any issues that would compromise the confidentiality and integrity of the ATS data stored on LinkedIn's platform. We can send copies of external penetration reports to our customers; ask your LinkedIn representative for more details.

a. **Internal Penetration Testing:** A dedicated penetration testing team is solely focused on ensuring code is designed, developed and deployed securely. All new products, features, major code refactoring and substantive changes to our platform have a security design review and application penetration test performed prior to being ramped to production.
b. **External Penetration Testing**: LinkedIn contracts with industry-leading security firms to perform annual web application penetration tests against core LinkedIn products, which includes manual and dynamic testing and source code analysis and review.

You can request to disable or delete your ATS data at any time.

If there is ever a time when you'd like to disable the Recruiter System Connect integration or remove this data, you can request to disable or explicitly delete your ATS data by contacting ltsatsintegrations@linkedin.com.

Upon the termination of the data processing services or upon your request, 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. Unless, legal requirements prevent LinkedIn from returning or destroying all or part of the customer's data shared with LinkedIn.

In short, we will retain your data for as long as we have an active contract, OR until you request for it to be deleted.

Protecting Your Data: Storage, disposal & beyond

You can use RSC in a GDPR-compliant way.

The goals of the GDPR are consistent with LinkedIn's longstanding commitment to data protection and transparency. To that end, RSC is built to enable customers to use it in a GDPR compliant manner. Customers are, of course, responsible for their own GDPR compliance.

Specifically, as with Recruiter in general, customers should get advice from their own counsel regarding GDPR compliance on:
1) Any personal data they may gather through Recruiter
2) Ensuring the provision of personal data to LinkedIn is consistent with their obligations under GDPR.

With regards to the **1-Click Export** feature of RSC, LinkedIn members control what they share with third-parties via the Privacy tab in their LinkedIn Settings. Therefore, we only show the 1-Click Export button for members that have not opted out from having their profile information (in the case of one-click export, their "stub profile" - name, headline, currently company, current title and general location) shared with third parties.

RSC also includes "delete" functionality that enables customers to satisfy data subject access requests for deletion. If a candidate were to request a customer to delete their data, the customer could delete that candidate's data from LinkedIn via the RSC "delete" API as integrated with their RSC-enabled ATS.

Specific GDPR help center here

Data is encrypted using NIST Special Publication standards.

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.

Additional resources:

General LinkedIn Resources:

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

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 alias for any technical support needs.

LinkedIn Recruiter System Connect