LinkedIn ATS Integrations

Data Security

Frequently Asked Questions

July 2025

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

What data is shared and why

Why does LinkedIn process ATS data?

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. The data synced to LinkedIn allows us to match candidates in your ATS to LinkedIn member profiles, and to surface information from your ATS in Recruiter so that you have all the up-to-date information about each candidate in one place.

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

We use only the data you've agreed to share, and your ATS determines the access permissions via your integration credentials. With your permission, LinkedIn retrieves recruiting-related data from your ATS. This includes:

- **Candidate data** (e.g. name, email, current status, candidate notes)
- **Application records** (e.g. job applied to, source, status history, application notes, resumes, interview feedback)
- **Job and requisition metadata** (e.g. job title, location, ID)
- **Application Stage and status history** (e.g. moved from "Phone Screen" to "Onsite")
- **Access Control Lists** (e.g. ACLs for restricting access to data that is access-controlled in your ATS)

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.

[In Beta, ATS Dependent] How will Hiring Assistant use and access my ATS data?

In 2026, we will be rolling out a new feature, ATS Connected Projects, that will allow you to connect your ATS job requisitions to LinkedIn hiring projects. This feature will allow you to view and manage applicants from your ATS on LinkedIn. If you have access to Hiring Assistant, you may enable it on a connected hiring project to allow Hiring Assistant to evaluate applicants from your ATS. Hiring Assistant will not be enabled on a project or have access to your ATS data without your consent.

Customers using ATS Connected Projects will also have the option to allow LinkedIn to update their ATS stages and application/candidate notes based on evaluation results. Outside of this option within ATS Connected Projects, RSC does not update your ATS data.

Who has access and how your data is protected

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.

How will my ATS Data be managed by LinkedIn?

- We will leverage your ATS data to power features in Recruiter that help save you time when you source, evaluate, and manage candidates on LinkedIn. **We will not make your ATS data available to other customers**. We may use aggregated, de-identified data to generate industry benchmarks and talent insights when those insights enhance your product experience. **We don't use your ATS data to create or add new LinkedIn profiles** or to modify any existing LinkedIn member profiles.
- You may ask us to delete your data at any time. Once your data is purged, it will no longer be stored or surfaced anywhere in your Recruiter experience.
- ATS data is processed with security measures in place and in compliance with your instructions. **You control your RSC data, while LinkedIn is the data processor**. The data is processed with security measures in place and in compliance with customers' instructions.

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

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 Site Reliability Engineers and Database Administrators 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 and reviewed 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.

What will LinkedIn do with my data outside of powering RSC?

We will use the data 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 would no longer use that data to improve our algorithms, but any improvements we made to general algorithms based on that data would persist.

Note: if you have the ATS-enabled Reporting package enabled, your LinkedIn account team will be able to view all LinkedIn Recruiter reports that are powered using this data in order to help you optimize your hiring strategy.

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.
3. We may use aggregated, de-identified data to generate industry benchmarks and talent insights when those insights enhance your product experience.

Resume data

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.

For Hiring Assistant customers (In Beta, ATS dependent)**: ATS Connected Projects** leverages resume data to allow Hiring Assistant to evaluate applicants from your ATS alongside those sourced on LinkedIn.

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 data 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.
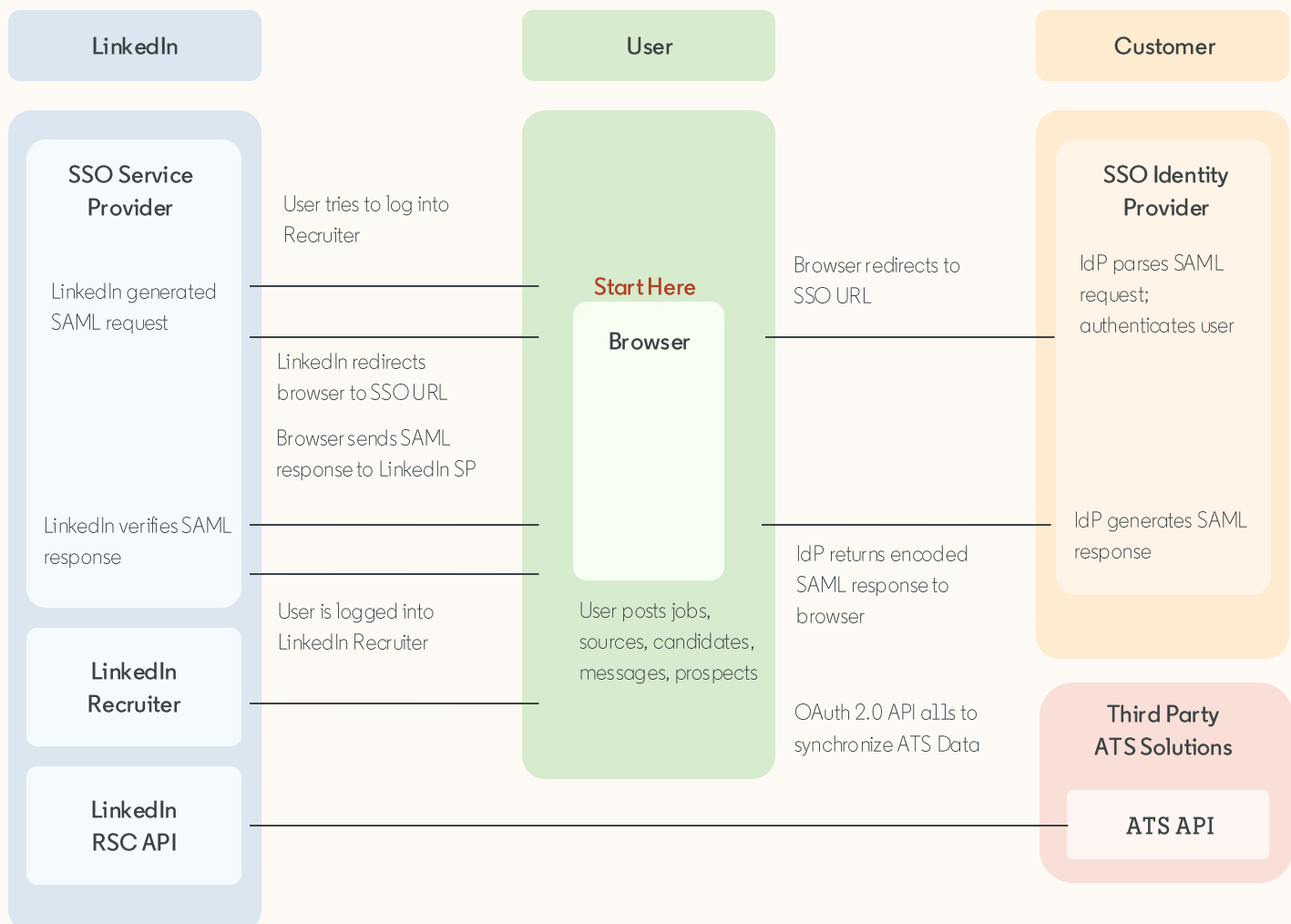
LinkedIn and your ATS: Bridging your data

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	User	Customer

SSO Service Provider

LinkedIn generated SAML request

LinkedIn verifies SAML response

LinkedIn Recruiter

LinkedIn RSC API

User tries to log into Recruiter

LinkedIn redirects browser to SSO URL

Browser sends SAML response to LinkedIn SP

User is logged into LinkedIn Recruiter

Start Here

Browser

User posts jobs, sources, candidates, messages, prospects

Browser redirects to SSO URL

IdP returns encoded SAML response to browser

OAuth 2.0 API calls to synchronize ATS Data

SSO Identity Provider

IdP parses SAML request; authenticates user

IdP generates SAML response

Third Party ATS Solutions

ATS API

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.
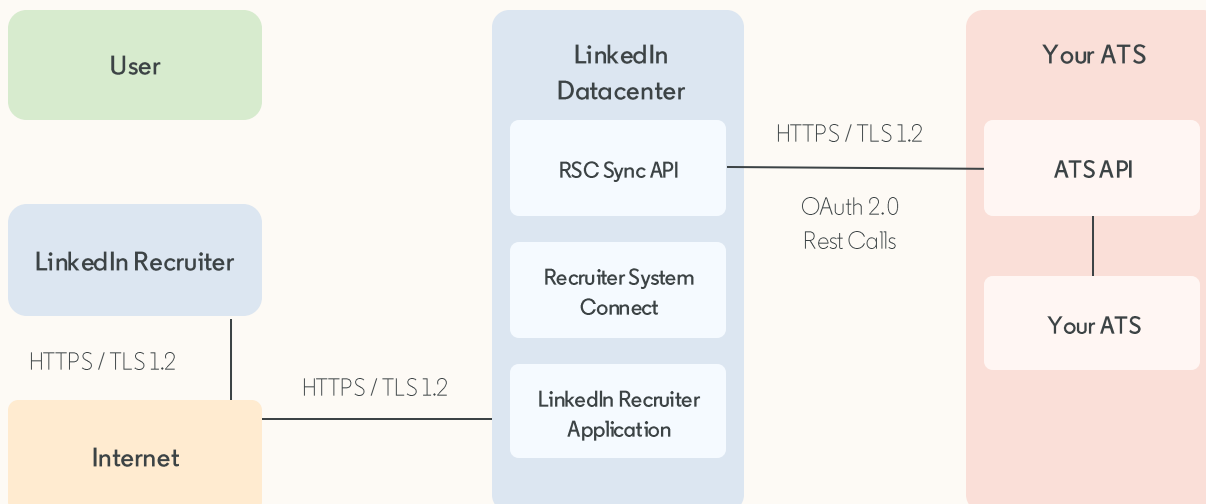
How are APIs authorized and protected?

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) or in-product.
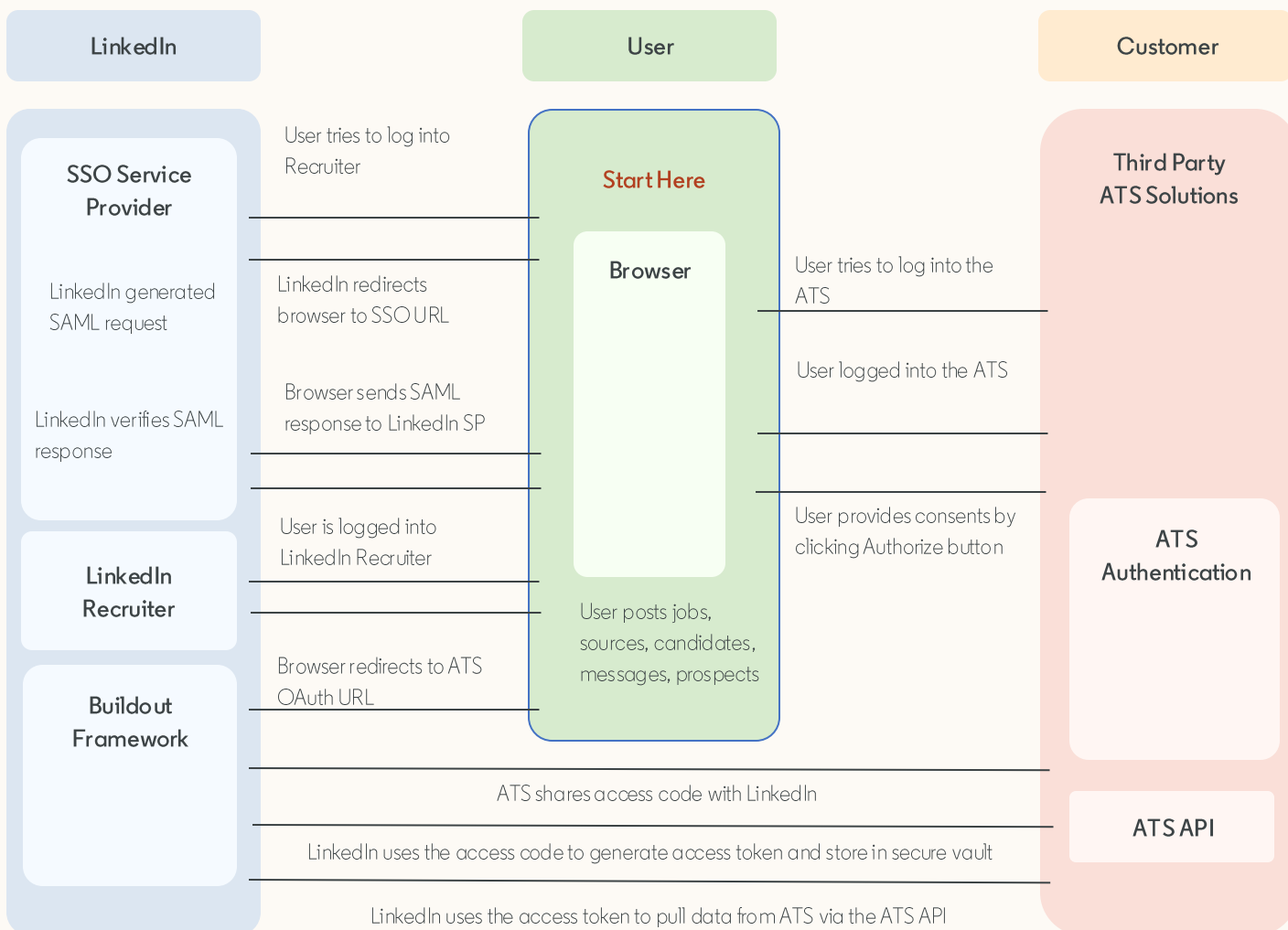
User	LinkedIn Datacenter	Your ATS
	RSC Sync API	ATS API
LinkedIn Recruiter	Recruiter System Connect	
	LinkedIn Recruiter Application	Your ATS
Internet		

HTTPS / TLS 1.2

HTTPS / TLS 1.2

HTTPS / TLS 1.2

OAuth 2.0 Rest Calls

LinkedIn and your ATS: Bridging your data

Authorizing "Enhanced Data Sync" allows LinkedIn to use ATS API calls to continuously monitor and improve data quality in RSC, retrieving data from your ATS and merging it with existing RSC ATS data to correct inconsistencies. All security measures, data processing and storage mechanics remain the same. Previously, your ATS sent data to LinkedIn through an integration with LinkedIn's API. In addition, LinkedIn can now pull data directly from your ATS when you authorize connecting through your ATS's credentials (OAuth token or API Key). RSC records may be retroactively changed, but we will not delete historical records unless you request deletion.

LinkedIn Talent Solutions and RSC Data Flow - "Enhanced Data Sync" authorization

This diagram provides a high-level logical overview of the SSO login and data-flow after authorizing "Enhanced Data Sync"

LinkedIn	User	Customer
SSO Service Provider	**Start Here**	**Third Party ATS Solutions**

User tries to log into Recruiter

Browser

User tries to log into the ATS

LinkedIn generated SAML request

LinkedIn redirects browser to SSO URL

User logged into the ATS

LinkedIn verifies SAML response

Browser sends SAML response to LinkedIn SP

User is logged into LinkedIn Recruiter

User provides consents by clicking Authorize button

LinkedIn Recruiter

ATS Authentication

User posts jobs, sources, candidates, messages, prospects

Browser redirects to ATS OAuth URL

Buildout Framework

ATS shares access code with LinkedIn

ATS API

LinkedIn uses the access code to generate access token and store in secure vault

LinkedIn uses the access token to pull data from ATS via the ATS API

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.
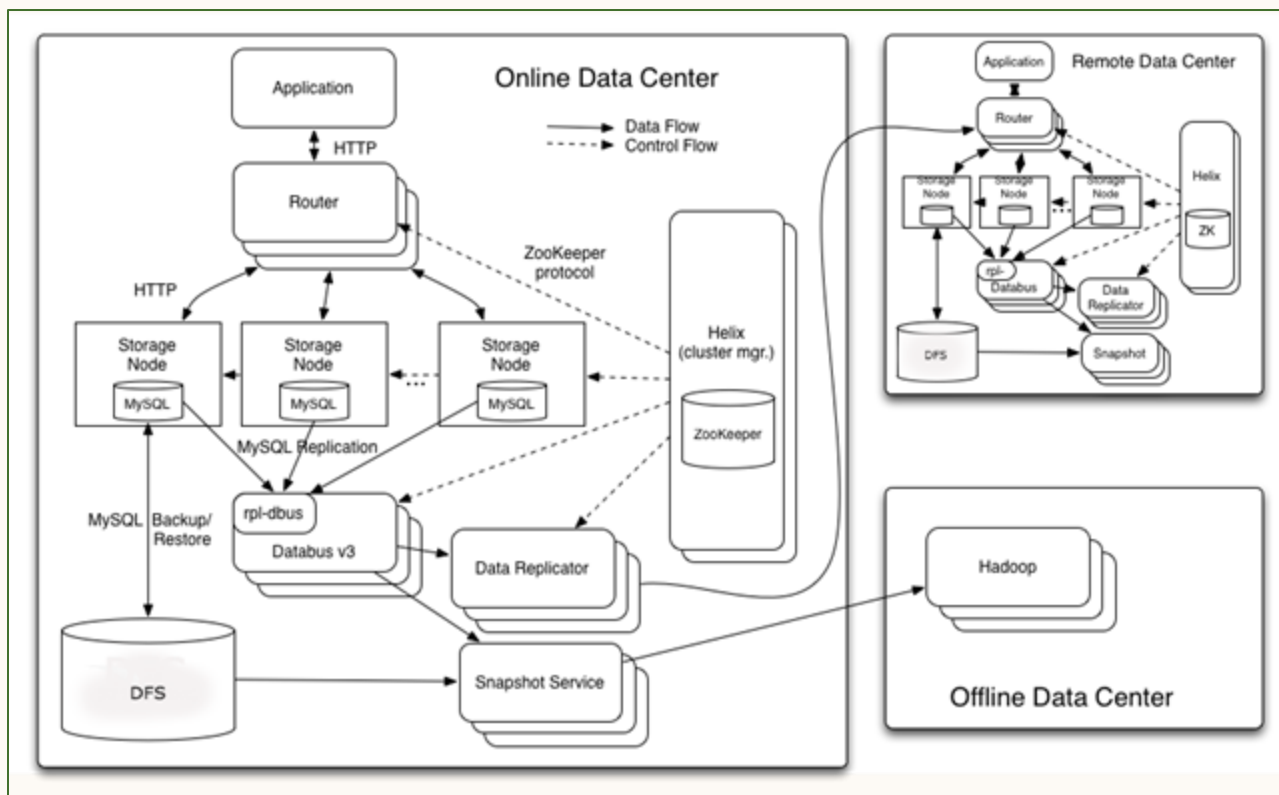
Storage, disposal & beyond

What security practices does LinkedIn use to protect my data?

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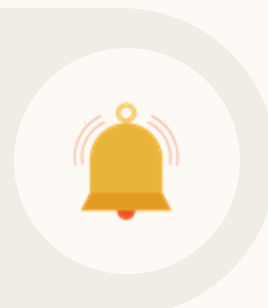
What happens if a LinkedIn member deletes their account after I have exported their data into my ATS using 1-Click Export?
You will receive notice so you can make an informed decision regarding the LinkedIn member data you have exported to your ATS records, and to help ensure that you are aware of our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

How do member-level privacy settings impact my ability to export candidates to an ATS or CRM?

LinkedIn is a members first organization and will always respect the privacy and settings of a member. Some members you try to export may have a setting selected on their profile that doesn't allow their information on LinkedIn to go to third-parties. We value the privacy of our members, so we won't allow their information to be exported through RSC or CRM Connect if they've selected this setting.

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?

General LinkedIn Resources are below:
- 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.