LEVER PRIVACY DATA SHEET

LEVER OVERVIEW

Lever is a talent cloud management software platform accessible to users via a web interface. Candidates providing personal data to a Customer will generally navigate to a Customer's website and submit a job application through the Customer website which will flow into the Customer's instance of the Lever platform. When a candidate provides personal data through the Customer's website that flows into the Lever platform, the Customer's privacy policy will govern the interaction between the candidate and the Customer. Lever will manage the applicant process, providing functionality to manage the interaction between the candidate and the Customer, track the candidate through application stages, seek feedback from a Customer's employees regarding a candidate, make hiring decision and send an offer letter. Lever provides a number of other integrations to enable additional functionality with systems such as email, background checks, employee onboarding, and HRIS.

Lever acts as a GDPR data processor for its customers ("Customers"), and provides comprehensive Data Protection Program and GDPR related product functionality to allow Customers to best meet their compliance needs. Lever enters into standard contractual clauses for purposes of lawful transfers of personal data outside of the European Economic Area.

PERSONAL DATA PROCESSING

Due to the nature of our product, Lever retains Personally Identifiable Information (PII) common to the process of fielding job applications. For candidates in our system, Lever commonly stores: name, email address, home address, telephone number, employment and education information, grades, salary, or job position. For employees using our services to manage the hiring process, Lever commonly stores: name, email address. Lever recommends Customers not request health data, legal data, credit card or bank account information as part of a hiring process.

Nature and Purposes of Processing:
Lever processes data for the purpose of enabling candidate relationship management, administering hiring and managing candidate evaluation processes. Personal Data will be subject to the following basic Processing activities: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject Categories
Lever stores the information of a customer's employees, a customer's candidates, and a candidate's references. Lever may store other data subject categories that a customer elects to enter into the Lever platform.

Categories of Data
Categories of data generally processed by Lever include:

- first name;
- last name;
- email address;
- address;
- employment history;
- location; and
- other information that may be requested by a customer or submitted by a candidate as part of a hiring process

Lever recommends a customer only request information required as part of the candidate evaluation process as required under Article 5, section 1(c) (data minimization).

Special categories of data

Lever does not recommend that customers collect special categories of personal data. These categories of information are generally not required during a candidate application process. Once a hiring decision is made, special categories of information required for employment can be requested as part of a new hire onboarding process.

CROSS BOARDER TRANSFERS

Standard Contractual Clauses
Lever maintains compliance with the GDPR for data transfers out of the EEA through standard contractual clauses. Standard contractual clauses are incorporated by reference to each Lever agreement as a standard practice; however, they can be removed at the request of the customer.

Sub-processors
Lever carefully selects services based on their security and availability. Lever performs due diligence on the technical and organizational security measures of all sub-processors, requires each to commit to obligations regarding their security controls and applicable regulations for the protection of personal data, and maintains a lawful transfer mechanism with each sub-processor as required by the GDPR. Lever will provide customers with at least fifteen days advance notice of the addition of new sub-processors. Lever's sub-processors are listed at www.lever.co/subprocessors

SECURITY

Security Framework
Lever has adopted a security framework aligned to ISO27001 and NIST for purposes of maintaining commercially reasonable security safeguards.

SOC 2 Type II
Lever participates in a third-party SOC 2 audit at least annually. Our most recent SOC 2 Type II report is available under NDA.

Penetration Testing
Lever participates in a third-party penetration test at least annually, testing both the external infrastructure and the web-based application for vulnerabilities. Our most recent penetration test results are available under NDA.

Contract Commitments
Lever's standard agreements includes a security exhibit that includes Lever's minimum security commitments located at www.lever.co/security-exhibit

PLATFORM DATA PROTECTION FUNCTIONAILTY

Access Control
Lever supports three models to authenticate (log in) to the application:

1. Lever-hosted username and password
2. Sign in with Google or Microsoft (OAuth)
3. Single Sign-On (SAML)

Lever-hosted credentials are encrypted at rest with 256-bit Advanced Encryption Standard (AES-256). Whenever users create a password for a Lever-hosted login, Lever reinforce password security best practices such as minimum character length, mixed use of letters, numbers, and special characters, and user feedback of password strength.
Lever does not store login credentials with OAuth- or SAML-based authentication. Temporary login access tokens are created using SHA256 and never stored. Lever's Audit API tracks failed sign-in attempts and requests for password recovery flows to monitor break-in attempts. (Requires purchase of Lever Audit API)
Connecting Lever to your identity management system allows you to centrally administer access and programmatically provision users to Lever.

Consent and Legitimate Interest
Lever supports functionality to allow customers utilize legitimate interest or consent to process candidate data. For customers that rely on candidate consent as the lawful basis for processing candidate personal data, Lever allows you to generate ‘Consent links’; URLs that direct each candidate to a unique page where they are prompted to update their consent.

Data Deletion Requests and Access Requests
Lever provides functionality to allow candidates to update their consent status, request a copy of their data, or request deletion of their data, all using a consent link that is unique to that candidate that may be accessed at any time by the candidate without requiring manual activity by a customer. Requests for deletion trigger a candidate to be flagged for anonymization, allowing a customer to comply with their obligations under the GDPR. More information on configuring Lever for GDPR consent is available here: https://help.lever.co/hc/en-us/articles/360002896652-How-do-I-reach-out-to-candidates-to-collect-or-refresh-consent-

Anonymization and Data Retention
Lever provides anonymization functionality that allows a customer to anonymize candidate data, rather than delete candidate data, preserving important insights for improved reporting. Customers may use IP addresses to geo-locate a candidate’s location when submitting an application and set appropriate retention timeframes for a candidate based on location. Retention timelines will flag candidates for anonymization at the end of the set timeframe and allow the customer to anonymize candidates individually or in bulk.