Candidate Data Privacy Policy
DataStax, Inc.

Last updated date: October 21, 2024

1. Introduction and Terminology

This Candidate Data Privacy Policy ("Policy") explains how DataStax treats the Personal Data it receives from and processes about its Candidates (also referred to in this Policy as "you"). This Notice applies to DataStax and to our controlled affiliates and subsidiaries ("DataStax" "we", "our" or "us"). A DataStax entity may collect or process Personal Data on behalf of another DataStax entity. If you are hired for employment in certain jurisdictions, a separate privacy policy may cover how we treat Personal Data in the employment relationship. For the purpose of this Policy, the relevant DataStax entity is the entity with whom you have applied for a position.

California Candidates can review our data collection, use, and disclosure practices and rights related to their Personal Data in the Supplemental Candidate Privacy Policy provided below .

If you are applying for a role at DataStax and you have any questions in relation to this Policy, please contact: legal@datastax.com.

In this Policy, the capitalized terms listed below have these meanings:

- "DataStax" means the entity to whom you have applied such as DataStax, Inc., or any of its subsidiaries.
- "Personal Data" means any information relating to a natural person who can be identified directly or indirectly from that information (in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person).
- "process", "processed", "processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as 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.
- "Candidate(s)" means anyone who applies for a job role or who otherwise provides or discloses Personal Data as they seek to carry out work with or for a DataStax Group company whether on a permanent or non-permanent basis.
- "Candidate Data" means any Personal Data relating to a Candidate.
- "Staff" means current and past employees, temporary staff, agency staff, and interns, including contractors employed or engaged by a DataStax Group company.

2. Collecting and Processing Candidate Data

DataStax, Inc., together with its subsidiaries and affiliates, respects an individual's right to privacy and values the confidentiality of Candidate Data.

DataStax processes Candidate Data as necessary for the recruitment and HR processes in the legitimate interests of DataStax, and the data will be transferred to DataStax's businesses and/or third parties

outside of the UK or European Economic Area where necessary for such purposes and subject to compliance with applicable legal requirements.

3. Our Collection of Candidate Data

Information that we collect automatically

When Candidates can visit the recruitment section of our website https://www.datastax.com/company/careers ("Careers Website") and search for jobs we automatically collect certain internet or other electronic network activity or information from your browser or device, through our use of cookies, web beacons, and similar technologies.

We use these technologies on our Careers Website to help us collect the data necessary to operate and manage our business. This includes analyzing and measuring device, browser, and system usage, detecting and preventing illegal, fraudulent, or unauthorized activity, enforcing our policies, and protecting our devices, systems information, and infrastructure. The information we collect using these technologies includes Personal Data, such as IP address and device information along with information related to the pages you visit, the links you click on, usage and crash information, as further described in our Collection notice within our Sites and Service Privacy Policy ("Sites and Services Privacy Policy") as Internet and Other Electronic Network Activity. Please see our Sites and Service Privacy Policy to understand how we use Personal Information collected via these technologies. And, review the Choice and Control of Personal Data section below on how you can manage your choices.

Personal Data collected from you

We collect the following categories of Personal Data about Candidates:

- Identification and contact details: name, home address, telephone number, email address
- Demographic information (including characteristics of protected classifications under applicable law): gender, date of birth, marital status, military or veteran status, social media information
- Professional or Employment Data:
    - Work and educational history, professional certificates and registrations;Details of your nominated referees (including their name, contact details, employer and job role);Details of your immigration/visa status;Previous applications/roles (information relating to previous applications you have made to DataStax Group companies and/or any previous employment history with a DataStax Group company;Other information you voluntarily provide throughout the process, including through correspondence with us, assessment centers, exercises and interviews.

We also may generate or derive inferences from any of the information identified in this Policy to create a profile about a Candidate reflecting a Candidate's preferences, characteristics, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes ("Inferences").

We may also use AI and automated technologies to collect information about you as part of our pre-screening process. For further information see section below on *Use of AI and automated technologies in our recruitment process.*

We collect the following categories of sensitive or special categories of Personal Data such as the following ("Sensitive Personal Data"):

- Government issued identifiers, such as national insurance, social security, or other government-issued identifying details, nationality and passport information; DMV driving records;
- Account log-in, in combination with a security or access code, password, or other credential that allows access to your online account;
- Sensitive demographic information that reveals your racial or ethnic origin, religious, political or philosophical beliefs or trade union membership; or
- information concerning your health or sex life (such as medical conditions related to pregnancy as part of an accommodation request), where authorized by law or where necessary to comply with applicable laws.

We ask that you only provide us with Sensitive Personal Data when such information is requested. ,For example, we may need to collect, or request on a voluntary disclosure basis, some Sensitive Personal Data for legitimate recruitment-related purposes for the purposes of equal opportunities monitoring, to comply with anti-discrimination laws and for government reporting obligations; or information about your physical or mental condition to consider accommodations for the recruitment process and/or subsequent job role. You may provide, on a voluntary basis, other Sensitive Personal Data during the recruitment process.

Personal Data collected from other sources

In addition the Personal Data we collect from you we collect the following categories of information (where permissible and in accordance with applicable law) from other sources:

• Directly or automatically collected from you or your browser, device
• Inferences we may derive from information we have collected
• Service providers (e.g., expense reimbursement services, cookies and similar technologies related to our providers' services)
• References provided by referees
• Other background information provided or confirmed by academic institutions and training or certification providers
• Criminal records data obtained through criminal record checks (where permitted or required by local laws)
• Information provided by recruitment or executive search agencies
• Information collected from publicly available sources, including any social media platforms you use or other information available online

4. How do we use or process Candidate Data?

We will use and process Candidate Data to administer and manage all aspects of our recruitment and hiring process, to assess whether you are suitable for the role for which you have applied, and for the categories of operational, business, safety, and security purposes described below.

Human Resources Uses:

- Recruitment and hiring assessment decisions;
- Interview travel and expense reimbursement processing;

- Benefits eligibility determination;
- Right to work eligibility determination (in applicable geographies);
- Equal employment opportunity, diversity, inclusion and accessibility programs;
- Legal and policy compliance administration and enforcement, including for the purpose of anti-discrimination laws and government reporting obligations.

Operational, Business, Safety, and Security Purposes

- Managing, monitoring, measuring, analyzing. protecting, and improving, our Systems, assets, and resources, including managing and protecting unauthorized access and use of company, personal, and customer data, devices, systems, and infrastructure; and protecting our Systems from intrusions;
- Managing, monitoring, measuring, analyzing, protecting, and improving campus, parking, buildings, office space, conference rooms, facilities, catering and café services, including monitoring and administering building occupancy and campus parking and transportation; operating and monitoring physical security systems, such as CCTV, key card entry systems, and guest logs; registering personal vehicles and logging exit and entry times; and emergency notification services;
- Managing and improving workplace, recruiting, and hiring efficiency and effectiveness;
- Communications and collaboration;
- Personalization to understand your preferences to enhance your recruitment and hiring experience;
- Using automated decision-making systems to analyze application information to assess your suitability for a role against the role requirements or description and to improve our recruitment processes and experiences;
- Delivery of information, goods, and services related to your application and recruitment;
- Research and improvement of our Systems, processes, products, services, and technology;
- Legal and policy compliance administration and enforcement, including monitoring access and use of our Systems.

Finally, we may use de-identified information in accordance with applicable law.

We process Candidate Data in accordance with applicable data protection laws. If you are accepted for a role at DataStax, the information collected during the recruitment process will form part of your ongoing staff member record and will be processed in accordance with our Staff Data Fair Processing Notice and Privacy Policy.

5. Disclosures of Candidate Data

Your Personal Data will be disclosed to and processed by certain HR staff, which may include line managers and other employees of DataStax where their role requires such access. We also use various providers to process Candidate Data as part of our recruitment and hiring processes.

We disclose Personal Data, including Sensitive Personal Data to the following categories of recipients:

•Our subsidiaries and affiliates, such as where we share business processes and common data systems Recruitment agencies, external training or testing providers involved in your recruitment;
• Service providers, vendors, or agents working on our behalf, including background checking or other screening providers and relevant local criminal records checking agencies; data storage, IT hosting and maintenance providers in relation to our recruitment and careers website/portal and providers of

automated solutions or AI tools that we may use to assist pre-screening as part of our recruitment process;
• Independent providers who can provide support and advice including in relation to legal, financial/audit, management consultancy, insurance, health, safety, and whistleblowing/reporting issues.
• Parties to a corporate transaction or proceeding, such as a a merger, financing, acquisition, bankruptcy, dissolution, or a transfer, divestiture, or sale of all or a portion of our business or assets.
• The general public, such as when we provide features or services that permit Candidates to publicly display or disclose certain Personal Data, such as a name or username, profile or directory information, or other Personal Data that you choose to disclose.
• Law enforcement ant those with legal necessity, such as where we disclose Personal Data to comply with applicable law or respond to valid legal process , including from law enforcement or other government agencies, and to operate and maintain the security of our systems, including to prevent or stop an attack on our systems or network, to protect protect the rights or property or ourselves or others, including enforcing our agreements, terms, and policies, or act in urgent circumstances such as protecting the health or personal safety of a candidate, employee, worker, agent, customer, user of our services, or member of the public.

We may disclose de-identified information in accordance with applicable law.

We disclose Candidate Data relating to Candidates from the European Economic Area, United Kingdom (UK), or Switzerland on lawful grounds including:

• Where you have provided your consent;
• To pursue our legitimate interests;
• The processing is necessary for the performance of a contract to which the you are party or in order to take necessary and appropriate steps prior to entering into a contract;
• To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant;
• In response to lawful requests by public authorities (including for tax, immigration, health and safety, national security or law enforcement purposes);
• As necessary to establish, exercise or defend against potential, threatened or actual legal claims;
• Where necessary to protect your vital interests or those of another person; and/or

We implement appropriate technical and administrative measures designed to ensure Candidate Data disclosed to another party is used in a manner consistent with this Policy.

In some cases, the disclosures described above may result in Candidate Data being transferred to a country that may have data protection laws that are different to the laws of the country in which you are located.

Specifically, our group companies, affiliated companies and providers operate around the world. This means that when we collect Candidate Data we may process it in any of these countries. Specifically, our parent company is based in the U.S. However, we have implemented safeguards designed to protect Candidate Data in accordance with this Policy and applicable data protection laws. This includes implementing the appropriate standard contractual clauses within the DataStax Group companies and providers, where applicable. Details of our standard contractual clauses can be provided upon request.

6. Choice and Control of Personal Data

We provide a variety of ways for you to control the Personal Data that we hold about you, including choices about how we use that data. In some jurisdictions, these controls and choices may be enforceable as rights under applicable law**.**

Communications preferences. You can choose whether to receive optional communications from us by email, SMS, and telephone related to future jobs or roles that become available. If you receive these optional communications from us and would like to stop receiving them, you unsubscribe by following the directions in that message or by contacting us as described in the "Contact Us" section below. If you receive a call from us related to new jobs or roles that become available, and no longer wish to receive such calls, you can ask to be placed on our do-not-call list. These choices do not apply to certain informational communications, including communications about an existing application with us.

Targeted advertising**.** To opt-out from or otherwise control targeted advertising, you have several options. You can use the controls available through our website cookie banner (where available) to decline advertising-related cookies. Or, you can use the opt-out controls offered by the organizations our advertising partners may participate in, which you can access at:

- United States: NAI (http://optout.networkadvertising.org) and DAA (http://optout.aboutads.info/)
- Canada: Digital Advertising Alliance of Canada (https://youradchoices.ca/)
- Europe: European Digital Advertising Alliance (http://www.youronlinechoices.com/)

Finally, you can use the other cookie controls described above. For more information about behavioral advertising cookies and about how to turn these features off please refer to the information available here or here.

Browser or platform controls.

Cookie controls. Most web browsers are set to accept cookies by default. If you prefer, you can go to your browser settings to learn how to delete or reject cookies. If you choose to delete or reject cookies, this could affect certain features or services of our website. If you choose to delete cookies, settings and preferences controlled by those cookies, including advertising preferences, may be deleted and need to be recreated. You can manage your cookie preferences through our Privacy Preference Center, which you can access on our website at www.datastax.com and selecting the "Cookie Settings" link at the bottom of the page.

Do Not Track. Some browsers include a "Do Not Track" (DNT) setting that can send a signal to the websites you visit, indicating you do not wish to be tracked. There is no common understanding of how to interpret the DNT signal; therefore, *our websites do not respond to browser DNT signals*. Instead, you can use the range of other tools to control data collection and use, including the cookie controls and advertising controls described above.

Email web beacons.

Most email clients have settings that allow you to prevent the automatic downloading of images, including web beacons, which avoid the automatic connection to the web servers that host those images.

7. Legal basis for processing European, Swiss and UK Candidate Data

Under European data protection law, our legal basis for processing Candidate Data as part of the recruitment process is:

- Our legitimate interests to manage the recruitment and hiring process and assess candidates for roles;
- To comply with applicable immigration and/or employment laws and regulations;
- To take steps prior to entering into an employment contract with a Candidate;
- In circumstances where the Candidate has made the data public;
- Where DataStax has the Candidate's consent to do so. Where consent is requested to process Personal Data, you have the right to withdraw your consent at any time;
- To protect the rights and interests of the DataStax Group, our employees, Candidates and others, as required and permitted by applicable law.

If we ask you to provide Personal Data to comply with a legal requirement or to perform a contract with you, we will make this clear to you at the relevant time and advise you whether the provision of Personal Data is mandatory or not (as well as the possible consequences if you do not provide your Personal Data).

If you have any questions about or need further information concerning the legal basis on which we collect and use your Personal Data, please contact us using the contact details in this Policy.

8. Retention of Candidate Data

Your Personal Data is kept throughout the recruitment process. If you are offered a position at DataStax then we will keep the Candidate Data obtained during the recruitment process and it will be retained and processed in accordance with our Staff Data Fair Processing Notice and Privacy Policy. If your application is unsuccessful we may keep your CV and other Candidate Data in accordance with our data retention obligations under applicable law as well as in accordance with applicable DataStax policies and may (for example, and where permitted by applicable law) contact you if another similar position arises. Please see the Choice and Control of Personal Data section above to learn more about how you can opt out of optional communications.

9. Use of AI and automated tools in recruitment process

As part of the recruitment process, we may use automated chatbots to carry out pre-screening interviews to determine whether you meet certain minimum objective criteria for a role you have applied for (e.g. number of years' experience). This will involve you being contacted by chat bot using the contact details provided to ask you questions about your work and educational history.

Based on your answers, the chatbot will assist us in assessing whether you meet the specific minimum criteria for that role. This minimum criteria for each role will have been made known to you as part of the job posting. Whether or not you meet these criteria will then determine whether or not your application progresses to the next stage. If you do not meet the minimum criteria, you will be informed of the outcome at the end of the pre-screening interview and your application will be rejected.

The questions are designed to avoid asking you to provide information about protected characteristics such as age or gender, or any questions that would require you to provide Sensitive Personal Data in response. However, there may be scenarios where you choose to provide such information. We have put measures in place to ensure such information will not be taken into account.

If the chatbot has trouble understanding your responses or is not working correctly, this will be flagged

and your application will be subject to human review.

Please note, you have the right to appeal decisions that we make in this way. If you wish to do so, then please contact us using the information set out in section 13 below.

Please note, you may also opt out of this process if you do not consider you are able to respond effectively to the chatbot. In such circumstances, you will be referred to a human reviewer to continue the pre-screening process.

10. Candidate Data Subject Rights for Candidates Outside the United States (US)

If our processing of Personal Data about you is subject to European Union, UK, Swiss, or other non-U.S. data protection law that provides you with certain rights with respect to your Personal Data, the following shall apply:

- You can request access to, rectification, or erasure of Personal Data;
- If any automated processing of Personal Data is based on your consent or a contract with you, you have a right to transfer or receive a copy of the Personal Data in a usable and portable format;
- If the processing of Personal Data is based on your consent, you can withdraw consent at any time for future processing;
- You can object to, or obtain a restriction of, the processing of Personal Data under certain circumstances;
- You have the right not to be subject to a decision based on automated processing of Personal Data, including profiling, if it produces a legal effect or similarly significantly affects you, unless such profiling is necessary for entering into or for the performance of a contract between you and us or we have you explicit consent; and
- For residents of France, you can send us specific instructions regarding using your Personal Data after your death.

Please use the contact information in the "Contact Us" section below to exercise one or more of these rights. You also have the right to complain to a supervisory authority, but we encourage you to contact us first with any questions or concerns.

To exercise any of these rights please contact: legal@datastax.com.

11. Privacy Rights for California Candidates

Under the California Consumer Privacy Act, or CCPA (Cal. Civ. Code 1798.100 et. seq.), and its amendments, including the California Privacy Rights Act of 2021, as a California resident you have certain rights regarding your Personal Data including rights to receive notice about how we process your Personal Data. For more information about how we process your Personal Data and your rights under CCPA, please review the Supplemental California Candidate Privacy Policy.

12. Changes to Candidate Data Privacy Policy

We may occasionally update this Policy to reflect changes as required by law or by our practices or procedures. If we make material changes to this Policy, or in how we use Personal Data, we will provide notice or obtain consent regarding such changes as may be required by law.

13. How to contact us

If you have any questions or concerns about this Policy, our collection or use of your Personal Data, please contact us using the following details.

Your country of residence	Email	Postal address
UK	privacy@datastax.com and legal@datastax.com	DataStax c/o Taylor Wessing 5 New Street Square London EC4A 3TW UK
EEA	privacy@datastax.com and legal@datastax.com	DataStax c/o: Fieldfisher Ireland The Capel Building Mary's Abbey Dublin D07 N4C6 Ireland
Rest of World	privacy@datastax.com and legal@datastax.com	DataStax, Inc. 2755 Augustine Dr 8th Floor Santa Clara, CA 95054, USA

Our UK representative is DataStax UK Limited. Our EEA representative is DataStax Ireland Limited. Our Data Protection Officer is Stuart Methven, privacy@datastax.com.

DataStax California Candidate Supplemental Privacy Policy

This DataStax California Candidate Supplemental Privacy Policy ("Supplemental Policy") supplements the DataStax Candidate Data Privacy Policy (" Policy") and further describes our collection, use, retention, and disclosure of Personal Data relating to our California Candidates.

This Supplemental Policy is designed to comply with the California Consumer Privacy Act of 2018, Civil Code section 1798.100 et seq as amended, including as by the California Privacy Rights Act of 2021 ("CCPA"). This Supplemental Policy is not intended to create any rights beyond those that exist by virtue of applicable California privacy and data protection law. Except as noted, all capitalized terms shall have the same meaning as in the Candidate Data Privacy Policy.

Collection of Personal Data

We collect Personal Data from you as described in our Candidate Data Privacy Policy.

Use of Personal Data

We use Personal Data that we collect from you as described in our Candidate Data Privacy Policy.

Retention of Personal Data

We retain Personal Data as described in our Candidate Data Privacy Policy.

Disclosure of Personal Data

We disclose Personal Data, including Sensitive Personal Data, to the following categories of recipients, for the following business purposes and as more fully described in the "Disclosures of Candidate Data" section of the Candidate Data Privacy Policy.

Category of Recipient and Purpose for Disclosure	**Categories of Disclosed Personal Data**
Our Subsidiaries and Affiliates.	● identification and contact details ● demographic information ● professional or employment data ● inferences ● internet or other electronic network activity information ● sensitive data

Service Providers, Vendors or Agents working on our behalf.	● identification and contact details ● demographic information ● professional or employment data ● inferences ● internet or other electronic network activity information ● sensitive data
Independent Parties.	● identification and contact details ● demographic information ● professional or employment data ● inferences ● internet or other electronic network activity information ● sensitive data
Parties to a Corporate Transaction or Proceeding.	● identification and contact details ● demographic information ● professional or employment data ● inferences ● internet or other electronic network activity information ● sensitive data
The General Public (such as where you choose to share such information).	● identification and contact details ● demographic information ● professional or employment data

Law Enforcement and Those with Legal Necessity.	• identification and contact details • demographic information • professional or employment data • inferences • internet or other electronic network activity information • sensitive data

Additionally, we sell or share Personal Data, including Sensitive Personal Data, with the following categories of recipients for the purposes described in this Supplemental Policy:

Category of Recipient	**Categories of Personal Information**
Advertising Providers	• inferences • internet or other electronic network activity information

Please see the "Choice and Control of Personal Data" and "Your Privacy Rights" sections below for more details.

Your Privacy Rights

Notice at Collection. At or before the time of collection, you have a right to receive notice of our privacy practices, including the categories of Personal Data and Sensitive Personal Data to be collected, the purposes for which such information is collected or used, whether such Personal Data is sold or shared, and how long such information is retained. You can find those details in this Candidate Data Privacy Policy, including this Supplemental Policy by clicking on the above links.

Right to Know. You have a right to request that we disclose the Personal Data we have collected about you. You also have a right to request additional information about our collection, use, disclosure, sale, or sharing of such Personal Data. Note that we have provided much of this information in our Privacy Policy and this Supplemental Policy.

Right to Request Correction. You have the right to request correction of inaccurate Personal Data.

Right to Request Deletion. You also have a right to request that we delete Personal Data under certain circumstances, subject to lawful exceptions.

To make a request to access, correct, or delete Personal Data, please submit requests as described in the Contact Information section below.

Right to Opt-Out. You have a right to opt-out from the "sale" or "sharing" of Personal Data, each of which are defined under CCPA.

Note that the CCPA defines "sell," "share," and "Personal Information" (referred to as "Personal Data" in both the Policy and this Supplemental Policy) very broadly, and some of our data disclosures described in the Candidate Data Privacy Policy and this Supplemental Policy may be considered a "sale" or "sharing" of Personal Data under those definitions. In particular, we let advertising and analytics providers collect IP addresses and cookie IDs when you access and use our applicant website or portal, but we do not "sell" or "share" any other types of Personal Data. Please review the Choice and Control of Personal Data section above for more information on how to opt-out from the sale or sharing of Personal Data. Or, You can manage your cookie preferences through our Privacy Preference Center, which you can access on our website at www.datastax.com and selecting the "Cookie Settings" link at the bottom of the page.

We do not knowingly sell or share the Personal Data of minors under 16 years of age.
Right to Limit Use and Disclosure of Sensitive Personal Data.
Where we use or disclose Sensitive Personal Data to infer individual characteristics characteristics or for purposes other than those permitted by CCPA, you have a right to request that we limit our use and disclosure of such Sensitive Personal Data.

We do not use or disclose Sensitive Personal Data for purposes of inferring individual characteristics or for additional purposes.

Right to Non-Discrimination. You have a right to not be discriminated against for exercising the rights set out in the CCPA.

Deidentified Information. When we retain aggregated or de-identified information for research purposes and to help us develop and improve our sites and services, we take reasonable steps to prevent reidentification of such personal information except where such reidentification is permitted under applicable law (such as where reidentification can help us determine whether our deidentification practices comply with applicable law).

Exercising Your Rights

Candidates may designate, in writing or through a power of attorney, an authorized agent to make requests on their behalf to exercise their rights under the CCPA. Before accepting such a request from an agent, we will require the agent to provide proof that you have authorized it to act on your behalf, and we may need you to verify your identity directly with us.

Further, to provide or delete specific pieces of Personal Data we will need to verify your identity to the degree of certainty required by law. We will verify a request by asking you to send it from the email

address associated with your application or by requesting additional information reasonably necessary to verify your identity.

Changes to This Supplemental Policy

We may occasionally update this Supplemental Policy to reflect changes as required by law or by DataStax practices or procedures. If we make material changes to this Supplemental Policy, or in how we use Personal Data, we will provide notice (or obtain consent) regarding such changes as may be required by law.

Contact Information

To submit a right to know, correction, deletion, or other privacy request, inquiry, or complaint, Candidates may contact the Privacy and/or Legal teams as follows:

- privacy@datastax.com
- legal@datastax.com