Confluent Candidate Privacy Notice

This Confluent Candidate Privacy Notice, including the EEA Supplement attached as Exhibit A, (collectively "Notice") describes how and when Confluent, Inc., and its group companies, collects, uses, and shares certain Personal Information (defined below) of job applicants and prospective employees located in California or the European Economic Area including the United Kingdom ("Candidate(s)"). This Notice does not address Confluent's privacy practices in relation to its employees, which are described in the *Confluent California Employee Privacy Notice* and *Confluent European Staff Privacy Notice*.

This Notice supplements the general information about our privacy practices available in our privacy statement.

Personal Information We Collect

In connection with your prospective employment or engagement with Confluent, we may collect, store, and use the following categories of information about you; this list is representative and not exhaustive. We refer to these categories as "Personal Information" throughout this Privacy Notice.

- **contact information and identifiers**, such as first and last name, online identifiers, account and usernames, aliases, IP address, email addresses, home and postal addresses, telephone numbers, and signatures;
- **facial images and audio information**, such as photos, videos and/or voice interactions or recordings;
- **demographic data,** such as age (including date of birth), gender, marital status, spouse and dependents, and certain sensitive data categories, described below;
- **professional and background information**, such as resumes/CVs, references, recommendations, academic and education background and qualifications, work skills and experience, professional certifications and registrations, language capabilities, training courses attended, results of criminal background checks, results of drug and alcohol testing;
- **work permit status**, such as immigration, residency, and related information;
- **benefits information**, such as information for determining benefits and cost estimation, (which may require information about gender, age, including birthdate, marital status, and Personal Information of spouse and dependents);
- **travel information**, such as dates and length of travel, hotel names and locations, travel routes and departures, stops, and destination points, and rewards earned for travel;
- **analytics or monitoring data,** including information required to access company systems and applications such as system ID, IP address, usernames, passwords, account details, device information, data necessary to facilitate proper operation,

and logs, or other information that you submit or input into our systems through completion of forms, and information about your use of our IT systems;

- **social media data,** including information posted in social media profiles and on recruiting websites, and user activity (posts, likes, replies, etc.);
- **public records,** including data or information publicly available online or through official governmental channels; and
- **sensitive data,** such as
  - government-issued identifiers including, social security, taxpayer identification, driver's license, and national/ID passport numbers;
  - criminal offenses;
  - information about legally protected classes; such as
    - race/ethnic and national origin;
    - religious creed;
    - physical, medical, or mental health or condition and related accommodations;
    - marital status;
    - gender;
    - age; and
    - sexual orientation where permitted by law and on the basis of voluntary and consensual disclosure.

In some circumstances we may anonymize your Personal Information so that it can no longer be associated with you or linked to you in any way. Anonymized data is not Personal Information and we may use such information without further notice to you.

Information Collection and Third Party Sources

We receive most Personal Information from you directly. For example, when you apply for a position at Confluent, we may collect Personal Information from your CV or resume, and through your interviews and correspondence with us.

We also sometimes receive Personal Information from third parties, including recruitment agencies, job boards, background check providers, social media and online searches (such as public databases and/or websites like LinkedIn, as permitted by law), former employers, and personal references. If you travel for a job interview or incur expenses in the recruitment process, we may also collect your Personal Information from our service providers (e.g., expense reimbursement services), or travel partners (e.g., travel agents and portals, car service, and ride share companies).

Purposes of Use

Confluent collects, uses, retains, and discloses Personal Information as appropriate to administer and carry out the recruitment and hiring process, and for operational, business, safety, and security purposes as described in this Notice.

For example, we may use your Personal Information to broadly evaluate how you fit into our organizational and hiring needs. We may also use systems application data to ensure network and information security, policy compliance, and to prevent fraud and abuse. Finally, we may use sensitive categories of data, such as Personal Information relating to your race, ethnic background, or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting, when legally required or permissible.

Purposes of Use	Categories of Personal Information
Human Resources Uses	
Recruitment and hiring decisions	Contact information and identifiers; facial images, and audio information; professional and background information; analytics or monitoring data; social media data; public records; sensitive data
Travel and expense reimbursements	Contact information and identifiers; travel information; analytics or monitoring data
Benefits eligibility determination	Contact information and identifiers; demographic data; benefits information; analytics or monitoring data, sensitive data
Equal employment opportunity, diversity, inclusion and accessibility programs	Contact information and identifiers; demographic data; sensitive data
Legal and policy compliance administration and enforcement (including for anti-discrimination laws and government reporting obligations)	Contact information and identifiers; facial images, and audio information; demographic data; professional and background information; work permit status; analytics or monitoring data, sensitive data
Business Uses	
Managing, monitoring, protecting, and improving, Confluent Systems, assets and resources, including preventing unauthorized	Contact information and identifiers; facial images, and audio information; demographic data; professional and background information; travel information; analytics or monitoring data; sensitive data

access and use of confidential information	
Managing, monitoring, protecting, and improving the Confluent workplace, including its facilities, on-site services, occupancy levels, security systems, and guest logs	Contact information and identifiers; facial images, and audio information; demographic data; professional and background information; personal vehicle information; travel information; analytics or monitoring data; sensitive data
Managing and improving workplace efficiency and effectiveness	Contact information and identifiers; facial images, and audio information; demographic data; travel information; analytics or monitoring data; sensitive data
Communications and collaboration	Contact information and identifiers; facial images, and audio information; demographic data; travel information; analytics or monitoring data; sensitive data
Delivery of information, goods and services	Contact information and identifiers; sensitive data
Legal and policy compliance administration and enforcement	Contact information and identifiers; visual, facial images, and audio information; demographic data; professional and background information; travel information; analytics or monitoring data; sensitive data
Research and improvement of Confluent processes, products, services, and technology.	Contact information and identifiers; visual, facial images, and audio information; demographic data; professional and background information; travel information; analytics or monitoring data; sensitive data

If you become a Confluent employee, Personal Information that was collected as part of the application and hiring process will become part of your employee file and will be used in the manner described in our employee privacy notices.

Sharing of Personal Information

We share Personal Information with your consent or for the purposes described in this Notice. For example, we share Personal Information with:

- **Our subsidiaries and affiliates,** including across business processes and common data systems;
- **Third party vendors or advisors working on our behalf,** including companies we've hired to provide recruiting, hiring, travel, and administrative services, systems providers, or third party vendors whose services or applications we otherwise use or rely on during the recruiting process;
- **As required by law or subpoena** or if we reasonably believe that such action is necessary to comply with the law or the reasonable requests of law enforcement, to enforce our Terms of Use or other agreements or to protect the security or integrity of our website, products, and services, and/or to exercise or protect the rights, property, or personal safety of Confluent, our staff, customers, users, or others.

We may also disclose Personal Information as part of a corporate transaction or proceeding such as a merger, financing, acquisition, bankruptcy, dissolution, or at transfer, divestiture, or sale of all or a portion of our business or assets.

How long do we keep your Personal Information?

If you are successful in your application your data will be kept in your personnel file. If you are unsuccessful, your data will normally be pseudonymized within six months after you have been informed that you were unsuccessful.

Changes to This Notice

Confluent may occasionally update this Notice to reflect changes in law or in Confluent's practices or procedures. If we make material changes to this Notice or how we use your personal Information, we will provide you notice of such changes or obtain your consent, where required by law.

Contact Information

Candidates may contact peoplesupport@confluent.io with any questions or complaints regarding Confluent's compliance with this Notice.

EXHIBIT A
EEA SUPPLEMENT

This Exhibit A, in conjunction with the Notice, is designed to comply with the General Data Protection Regulation ("**GDPR**"). This Exhibit A only applies to Personal Information originating from the EEA and is not intended to create any rights beyond those that exist under the GDPR or other applicable privacy and data protection laws.

Transfers of Personal Information outside the European Economic Area

When we transfer Personal Information from the European Economic Area (including the United Kingdom) and from Switzerland to the United States or other countries which have not been determined by the European Commission to have laws that provide an adequate level of data protection, we use legal mechanisms, including contracts, designed to help ensure your rights pertaining to your Personal Information are protected. Specifically, our website servers are located in the United States and our affiliates, partners, third parties and service providers operate in the United States, European Economic Area, Canada, India, and Australia. When we collect your Personal Information we may process it for the purposes detailed in the Notice, in any country that members of our group or third party data processors are located. We have taken appropriate safeguards to require that your Personal Information will remain protected in accordance with this Privacy Statement. The safeguard Confluent primarily relies upon is the European Commission-approved standard contractual data protection clauses. For more information about these mechanisms, please contact us using the contact details provided in the “Contact details” section in the Notice.

Legal grounds for processing Personal Information

What are the grounds for processing?

"Process" and "Processing" means any operation or set of operations which is performed on your Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In order to comply with European data privacy laws, we need to have legal bases for using your personal information for the purposes described in this Privacy Notice. In nearly all cases, our legal basis will be one or more of the following:

(a) our use of your personal information is necessary for the performance of our obligations under a contract with you (for example, to pay you, communicate with you, or confer benefits upon you); and/or

(b) our use of your personal information is necessary to comply with our legal obligations, including as your potential employer/engager (for example, by providing information to tax authorities, or conducting legally required work authorization checks); and/or

(c) our use of your personal information is necessary for the purposes of our legitimate interests or the legitimate interests of a third party (for example, to operationalize a group-wide company structure, information sharing, and internal reporting, to perform our obligations to customers and maintain good relations with them, to ensure a safe and secure working environment and prevent fraud or other harms, or in connection with corporate transactions such as mergers, acquisitions, or debt or equity financings); and/or

(d) less commonly, our use of your personal information is necessary to protect a person's vital interests, or to perform a task carried out in the public interest.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Processing sensitive Personal Information

Sensitive personal data, so called "special categories" of personal data, require higher levels of protection. Special category data is personal data relating to racial or ethnic origins; political opinions; religious and philosophical beliefs, trade union membership; genetic data; biometric data; health data; sex life or sexual orientation. We may process special categories of personal data with your explicit written consent. We may also process special categories of personal data when:

(a) It is needed to carry out our legal obligations and/or exercise certain legal rights (such as in the field of employment law);

(b) It is in the public interest (such as for equal opportunities monitoring or in relation to an occupational pension scheme);

(c) It has already been manifestly made public by you;

(d) It is needed to assess your working capacity on health grounds; or

(e) it is needed to protect a person's vital interests and you are not capable of giving your consent.

We may occasionally ask you for your consent to process certain sensitive data. Your consent is not a condition of your application with us and you may withdraw any consent given in such circumstance by contacting privacy@confluent.io.