Intercom

Privacy Notice for EU and UK Candidates

Effective Date: January 1, 2023

1. Introduction

Intercom, Inc., Intercom R&D Unlimited Company, and Intercom's group companies (**"Company", "we", "us" and "our"**) may operate in many different countries. Some of these countries have laws related to the collection, use, transfer and disclosure of the personal information of individuals, including job candidates. We take these obligations very seriously and are committed to protecting the privacy of our current and former candidates.

The purpose of this Privacy Notice for EU and UK Candidates (the "Notice") is to give job candidates who are based in the European Economic Area and United Kingdom ("EU and UK Candidates") information about what personal information we collect, how we collect, use and disclose that information, the legal grounds for us doing this, and their rights in respect of their personal information.

Intercom, Inc., Intercom R&D Unlimited Company, and Intercom's group companies collectively is the data controller of your personal information and is responsible for how your personal information is processed.

This Notice does not form part of your application or any future contract of employment and may be updated at any time. We will provide you with a revised Notice if we make any substantial updates. It is important you read this Notice, so that you are aware of how and why we are using your personal information.

2. What Information We Collect About EU and UK Candidates

Before, during and after their application to the Company, including time spent on the Careers section of our website ("Careers Site"), we may collect and process information about EU and UK Candidates. We refer to such information in this Notice as "EU and UK Personal Information." We collect the following EU and UK Personal Information:

- **Personal Details,** such as name, email, phone numbers, home address, languages(s) spoken, gender, date of birth, national identification number, emergency contact information and photograph;
- **Documentation Required under Immigration Laws,** such as citizenship and passport data, details of residency or work permit;
- **Talent Management Information,** such as details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications and memberships, language and other relevant skills, certification, certification expiration dates), information necessary to complete a background check, information relating to references such as referees' names and contact details, details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license information, and information used to populate employee biographies;
- **Any other information you provide to us,** such as current salary, desired salary, employment preferences; and
- **Sensitive Information,** such as EU and UK Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or data concerning a person's sex life or sexual orientation, disability status, and criminal conviction data. Data concerning health may include your body temperature, health symptoms and other screening information in connection with the Company's health and safety plans and protocols,

including screening required to access Company offices/facilities and other measures designed to prevent the transmission of COVID-19 or other infectious diseases.

We ask that you avoid submitting Sensitive Information, unless such information is legally required and/or the Company requests you to submit such information.

Any information you submit through the Careers Site must be true, complete and not misleading. Submitting inaccurate, incomplete or misleading information may lead to a rejection of your application during the recruitment process or disciplinary action including immediate termination of your employment. In addition, it is your responsibility to ensure that the information you submit does not violate any third party's rights.

If you provide us with personal information of a referee or any other individual as part of your application, it is your responsibility to obtain consent from that individual prior to providing the information to us.

3. Sources of EU and UK Personal Information

We collect EU and UK Personal Information from the following sources:

- **EU and UK Candidates** in person, online, by telephone, or in written correspondence and forms;
- **Third-party websites** where you can apply for jobs at the Company;
- **Previous employers and other referees** in the form of employment references;
- **Background and credit check vendors** as part of the recruitment process;
- **Employment agencies and recruiters**; and
- **Providers of sanctions and "politically exposed persons" screening lists**.

4. How we use and disclose EU and UK Personal Information

Legal Basis for Processing

We will only use EU and UK Personal Information when the law allows us to. Most commonly, we will use your EU and UK Personal Information in the following circumstances:

- where it is necessary in order to take steps at your request prior to entering into an employment contract;
- where it is necessary to comply with a legal obligation (including, in respect of Sensitive Information, obligations under employment law) on us; and
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example, the Company has a legitimate interest in conducting certain background checks on Candidates to ensure that it is offering employment to those individuals whom it considers are most likely to be successful when working for the Company.

We may also use your EU and UK Personal Information in the following situations, which are likely to be rare:

- where it is necessary to protect your (or someone else's) vital interests (and, in the case of Sensitive Information, where you are incapable of consenting);
- where it is necessary for us to defend, prosecute or make a claim against you, us or a third party; and
- in the case of Sensitive Information, where you have made the information public.

In particular, we may use your Sensitive Information, such as health/medical information, in order to accommodate a disability or illness during the recruitment process, and reduce the risk of transmission of COVID-19 or other infectious diseases should you be visiting the Company offices, your diversity-related EU and UK Personal Information (such as race or ethnicity) in order to comply with legal obligations relating to diversity and anti-discrimination, and your criminal conviction data only where it is appropriate (given the role for which you are applying) and we are legally able to do so.

Purposes of Processing

We process EU and UK Personal Information for the following purposes**:**

- **Managing Workforce:** Managing recruitment and assessing your suitability, capabilities and qualifications for a job with us, processing your application and performing background checks if we offer you a job, such as credit checks, anti-fraud checks and checks to prevent fraud and money laundering;
- **Communications:** Facilitating communication with you regarding your application;
- **Taking legal action:** Pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations and complying with internal policies and procedures; and
- **Compliance and safety:** Complying with legal (including, in respect of Sensitive Information, obligations under employment law) and other requirements, such as record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas. This includes complying with applicable public health guidelines and requirements related to the prevention and control of COVID-19 or other infectious diseases, as well as ensuring the health and safety of employees by controlling access to and monitoring our physical premises (e.g. by requiring health screenings to access Company offices/facilities).

There may be more than one purpose that justifies our use of your EU and UK Personal Information in any particular circumstance.

We will only use your EU and UK Personal Information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your EU and UK Personal Information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

If you fail to provide certain EU and UK Personal Information when requested, we may not be able to review your application, or we may be prevented from complying with our legal obligations.

Disclosures to third parties

We share EU and UK Personal Information with the following unaffiliated third parties:

- **Service Providers:** Companies that provide products and services to the Company such as human resources services, IT systems suppliers and support and background check providers, recruiters and headhunters, and hosting service providers; and
- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over the Company such as regulatory authorities, public bodies, and judicial bodies, including to meet national security or law enforcement requirements.

5. Transfer of EU and UK Personal Information

The Company may disclose EU and UK Personal Information throughout the world to fulfil the purposes described above. This may include transferring EU and UK Personal Information to other countries (including countries other than where an EU or UK Candidate is based and located outside the European

Economic Area ("EEA") and UK) that have different data protection regimes and which are not deemed to provide an adequate level of protection for EU and UK Personal Information. To ensure that EU and UK Personal Information is sufficiently protected when transferred outside the EEA and UK the Company has put in place protective measures.

6. Data Security

The Company will take appropriate measures to protect EU and UK Personal Information that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of EU and UK Personal Information.

Access to EU and UK Personal Information within the Company will be limited to those who have a need to know the information for the purposes described above, and may include personnel in HR, IT, Compliance, Legal, Finance and Accounting. Such personnel will generally have access to EU and UK Candidates' business contact information such as name, desired position, telephone number, postal address and email address.

The Company has put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach of your EU and UK Personal Information where we are legally required to do so.

7. Data Retention

The Company's retention periods for EU and UK Personal Information are based on business needs and legal requirements. We retain EU and UK Personal Information for as long as is necessary for the processing purpose(s) for which the information was collected, as set out in this Notice, and any other permissible, related purposes. For example, we may retain certain information to comply with regulatory requirements regarding the retention of such data, or in the event a litigation hold is imposed. When EU and UK Personal Information is no longer needed, we either irreversibly anonymise the data (and we may further retain and use the anonymized information) or securely destroy the data.

8. Data Accuracy

The Company will take reasonable steps to ensure that the EU and UK Personal Information processed is reliable for its intended use and is accurate and complete for carrying out the purposes described in this Notice.

9. Automated Decisions

The Company does not envisage that you will be subject to decisions that will have a significant impact on you based solely on automated decision-making. The Company will notify you in writing if this position changes.

10. Your Rights

You have the right, in certain circumstances, to object to the processing of your EU and UK Personal Information. You also have the right, in certain circumstances, to access your EU and UK Personal Information, to correct inaccurate EU and UK Personal Information, to have your EU and UK Personal Information erased, to restrict the processing of your EU and UK Personal Information, to receive the EU and UK Personal Information you have provided to the Company in a structured, commonly used and machine-readable format for onward transmission, and to object to automated decision-making. You may submit requests to exercise your rights through our Privacy Request Form or by mailing our Data Protection Officer at 55 2nd Street, 4th Fl., San Francisco, CA 94105, USA, Attention: Compliance. Please note that certain EU and UK Personal Information may be exempt from such access, correction, erasure, restriction and portability requests in accordance with applicable data protection laws or other laws and regulations.

You also can file a complaint with your local data protection supervisory authority. You can find your data protection authority here.

11. Your Obligations

You should keep your EU and UK Personal Information up to date and inform us of any significant changes to your EU and UK Personal Information.

12. Privacy Shield

Company has certified its compliance with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from the EU. Although no longer relying on the Privacy Shield to validate its international transfers, Company continues to adhere to and commit to apply the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability. If there is any conflict between the terms of this Notice and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

For purposes of enforcing compliance with the Privacy Shield, we are subject to the investigatory and enforcement authority of the US Federal Trade Commission. Intercom shall be liable in cases of onward transfers to third parties. Under certain circumstances, we may be required to disclose your personal data in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

For more information about the Privacy Shield, see the US Department of Commerce's Privacy Shield website located at: https://www.privacyshield.gov. To review our certification on the Privacy Shield list, see the US Department of Commerce's Privacy Shield self-certification list located at: https://www.privacyshield.gov/list and search for "Intercom, Inc.".

In compliance with the Privacy Shield Principles, Intercom commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Intercom through our Privacy Request Form or by mailing into 55 2nd Street, 4th Floor, San Francisco, California 94105, United States of America, Attention: Legal .

Company has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship.

You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: (1) raised your complaint directly with us and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified above; and (3) raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to you. To find out more about the Privacy Shield's binding arbitration scheme please see www.privacyshield.gov/article?id=My-Rights-under-Privacy-Shield.