Job Candidate Privacy Policy

Thank you for your interest in accessiBe ("**we**", "**us**", "**our**" or "**our Company**").

We put great effort into ensuring that we secure the personally identifiable information related to you ("**Personal Data**")[1] and use it properly.

This job candidate privacy policy ("**Policy**") describes how we use and protect Personal Data related to job candidates who apply for a position with us.

By reading this Policy, you can understand, among others, which Personal Data related to you we collect and use, how we use it, and what rights you have.

Please take the time to read and understand this Policy, which should be read in conjunction with our General Privacy Notice, applicable to the general use of our website and services.

If you do not consent to this Policy or the general Privacy Notice, do not forward your details or apply for a position at accessiBe.

1. **General**:

   When you, as a job candidate, interact with us, you agree that we will collect, store, and use Personal Data about you in the manners that are outlined in this Policy.

   We will only process the Personal Data related to you in ways that you would reasonably expect of us to provide a safe, legal, and efficient job application process.

   You are under no legal obligation to deliver any Personal Data. You agree, however, that without delivery of the Personal Data, we may be unable to assess your suitability for a position with us.

   U.S. state privacy laws. Some U.S. state privacy laws, such as the California Consumer Privacy Act (CCPA), require specific disclosures for state residents. In this Policy, we explain: (i) the categories of Personal Information we collect and the sources of that data; (ii) how we use Personal Information; (iii) when we may disclose Personal Information; and (iv) how we retain Personal Information.

[1] Data that has been de–identified, anonymized, or aggregated or that otherwise cannot reasonably be related back to a specific person is not considered Personal Data.

We do not sell your personal information. We also do not "share" your Personal Information as that term is defined in the CCPA. State laws like the CCPA also provide the right to request information about how accessiBe collects, uses, and discloses your Personal Information and the right not to be discriminated against for exercising these privacy rights.

EU or UK data protection. If EU data protection or UK data protection law applies to the processing of your Personal Data, our legal basis for processing your information is where it is necessary for the job application process. We also rely on your consent and may process information where it is necessary to comply with a legal obligation or for purposes connected to legal claims. We rely on a legitimate interest to improve our application or recruitment process.

2. **Automated Decision-Making**:

We may use a third-party service provider's technology to select appropriate candidates to consider based on criteria expressly identified by us or on what is typical about the role you have applied for. Nevertheless, you will not be subject to decisions that will significantly impact you based solely on automated decision-making.

3. **Types of Personal Data we Collect**.

When you apply for a job at our Company, we will need to process information about you (including Personal Data related to you) as necessary to assess your suitability for the relevant position.

The Personal Data that we will process for such purpose will include information that you provide when you apply for a position with us, for example:

- **Identification data** – such as your name, gender, photograph, and date of birth.
- **Contact details** – such as address, telephone number, and email address.
- **Background information** – such as academic/professional qualifications and experience, employment history, education, CV/résumé. Where permissible and in accordance with applicable law, criminal records data (for vetting purposes).
- **Government identifiers** – such as government-issued ID/passport, immigration/visa status, and social security number.

- **HR Records** – information related to your progress through any hiring process that we may conduct.
- **Sensitive Personal Data** - We may also process sensitive Personal Data relating to you. Sensitive Personal Data includes any information that reveals your racial or ethnic origin, religious, political, or philosophical beliefs, sexual orientation and information about your health ("**Sensitive Personal Data**"). In the United States, Sensitive Personal Data also includes government identifiers (including social security, driver's license, state identification card, or passport number), citizenship or immigration status, and precise geolocation data.

  As a rule, we try not to collect or process any Sensitive Personal Data about you, unless authorized by law or where necessary to comply with applicable laws or to provide benefits. We do not sell Sensitive Personal Data collected under this Notice. However, in some circumstances, we may need to collect, or request on a voluntary disclosure basis, some Sensitive Personal Data for legitimate employment-related purposes: for example, information about your racial/ethnic origin, gender and disabilities for the purposes of equal opportunities (on the basis that it is in the public interest and in accordance with applicable law), monitoring, to comply with anti-discrimination laws and for government reporting obligations, or information about your physical or mental condition to provide work-related accommodations.

4. **Sources of Personal Data**:

Usually, you will have provided the information we hold about you, but there may be situations where we collect Personal Data or Sensitive Personal Data from other sources. Such may include the following:

- Background and other information from recruitment agencies, background checking agencies, and other third parties during your recruitment, where permissible and in accordance with applicable law.
- Publicly available Personal Data about you (*e.g.* LinkedIn and other social media profiles).
- We may receive Personal Data from a third party who recommends you as a candidate.

We also use video cameras for our premises and store information captured by this equipment to secure its networks, systems, and property in accordance with applicable law.

Personal Data learned about you through online interviews and evaluations can include information about your personality, behaviour, and suitability for a particular position. Sensitive Personal Information may be revealed in a video interview. We do not require such information as part of these interviews. If you do not consent to your personal information being recorded or used as set out in this section, do not apply through this process.

5. **Purposes for Processing Personal Data**

We collect and use your Personal Data primarily for recruitment purposes – in particular, to determine your qualifications for employment and to reach a hiring decision. This includes assessing your skills, qualifications, and background for a specific role, verifying your information, carrying out reference or background checks (where applicable), and generally managing the hiring process and communicating with you about it.

We may also collect and use Personal Data when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently.

6. **With whom we Share your Personal Data**:

We allow access to Personal Data only to those who require such to perform their tasks and duties, and to third parties with a legitimate business purpose or other lawful ground for accessing it. Whenever we permit a third party to access Personal Data, we will implement reasonable measures to require the Personal Data be used in a manner consistent with this Policy and applicable law.

We will share your Personal Data in the following instances:

- We have offices in the US and in Israel and all services are cloud-based. Therefore, Personal Data related to job candidates will be shared between the two offices.
- With our relevant employees to facilitate your application and the job recruitment process.
- To the extent necessary for the recruitment process.
- With our third-party service providers, to help us with the recruiting process. Such third parties might maintain their terms of use and privacy policies for your use of those platforms, for which we disclaim any responsibility. For example:

- We use Comeet Technologies, Inc. as our third-party service provider to provide a platform for our recruitment process. Its Privacy Notice can be found at https://help.comeet.com/en/articles/3134994-privacynotice.
- Zoom to set up online job interviews. Its Privacy Statement can be found at https://explore.zoom.us/en/privacy/.
- DocuSign for electronic signatures of job offers. Its Privacy Notice can be found at https://www.docusign.com/privacy/.
- For US candidates **only**, subject to consent and applicable law, we use Certn for criminal background checks, its privacy notice can be found at: https://vault.pactsafe.io/s/5d800911-f26c-4e3a-884d-85117a81799b/legal.html?g=37964#contract-byeg-ihlj

- With a competent supervisory authority, if we believe doing so is in accordance or otherwise required by applicable law, regulation, judicial or legal process.
- With law enforcement or other authorities when it is necessary, in our reasonable opinion, to protect our interests or that of individuals.

7. <u>Where Personal Data is Maintained, Processed, and Stored</u>:

The main locations in which we will maintain, process, and store your Personal Data are the USA and Israel.

We are committed to protecting Personal Data in accordance with this notice, customary industry standards, and such appropriate lawful mechanisms and contractual terms requiring adequate data protection, regardless of any lesser legal requirements that may apply in the jurisdiction to which such data is transferred.

8. <u>Protecting your Personal Data</u>:

We maintain industry-standard technical and organizational measures for the protection of Personal Data (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss, or alteration or damage, and unauthorized disclosure of or access to Personal Data).

We limit access to your Personal Data to those with a genuine business need to know it. Those processing your information will do so only in an authorized manner and are subject to a duty of confidentiality.

We also have procedures to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your Personal Data, we cannot guarantee the security of your data transmitted through any online means, therefore any transmission remains at your own risk.

9. **Data Retention Periods**:

Personal Data will be stored in accordance with applicable laws and kept as long as accessiBe has an ongoing legitimate business need to carry out the purposes described in this Policy, or as otherwise required by applicable law. If you are offered and accept employment with accessiBe, the information collected during the application and recruitment process will become part of your employment record.

We also may retain and use your Personal Data where we consider it necessary for complying with laws and regulations, including collecting and disclosing Personal Data as required by law (*e.g.* for anti-discrimination and other employment laws), to protect vital interests or to exercise or defend our legal rights.

If we need to delete Personal Data related to you, it will take some time until we completely delete residual copies of said Personal Data from our active servers and from our backup systems.

10. **Your rights**:

You can contact us and request access to the Personal Data we keep about you. We may ask you for certain credentials to verify your identity.

If your Personal Data is inaccurate, incomplete, unclear, or not up-to-date, you can request the correction, amendment or deletion of such Personal Data. Any such request should be addressed to accesiBe's Talent Acquisition Team at the email stated below.

Under certain circumstances by law, you may have additional rights as a data subject. Please refer to the Privacy Notice or send us an email for further information.

11. **Contact**:

If you have any questions or concerns about this Policy or about the way we process Personal Data related to you, you are welcome to contact us at hrprivacy@accessibe.com.

12. <u>Updates to this Policy</u>.

This Policy may be updated periodically to reflect changes in our privacy practices or applicable law.

Last update: March 2024