PINDROP SECURITY
CANDIDATE PRIVACY NOTICE

Date: March 24, 2025

Summary of Key Points
To help you understand how we handle your personal data, here are the key highlights:

1. **Your personal data is collected to evaluate your job application** and includes resume details, interview recordings, and assessment results.
2. **The hiring process may include video/audio/data recording and monitoring;** the data recorded may constitute "biometric information" under specific state privacy and/or biometric laws.
3. **The data recorded will only be used** (1) for verification and fraud prevention (e.g. detect manipulated, synthetic or AI generated content, deepfakes); and (2) to train and improve the Pindrop models and tools used for verification and fraud prevention.
4. **Your data is stored primarily in the U.S.**, with safeguards for international transfers where required.
5. **We retain your data for up to six months** unless legally required to keep it longer or you consent to future job opportunities.
6. **You have rights over your data**, including access, correction, and deletion. Contact **privacy@pindrop.com** for requests.

For full details, please continue reading below:

---

1. Introduction

Pindrop Security and our affiliated companies (together, "Pindrop", "we", "our" or "us") values your privacy and is committed to protecting your personal data. When you apply for a job with us, we collect and process certain information about you to manage the hiring process. This notice explains what data we collect, how we use it, who we share it with, and the rights you have regarding your information.

If you are a California resident, please refer to the Additional Privacy Information for California Residents section below for information about the categories of information we may collect and your rights under applicable California privacy laws.

2. Personal Data We Collect

During the hiring process, we may collect the following types of personal data:

- **Basic details**: Your name, contact information, nationality, and work eligibility.
- **Employment and education history**: Your CV, references, qualifications, degrees, transcripts, institutions attended and any additional information you provide.
- **Assessments and interview data**: Results from skills assessments, including those conducted by external service providers, interview notes, and recorded interviews where applicable.
- **Recorded video, audio, and phone interviews**: Your interview may be recorded, including all video, audio, and other recordable data, and Pindrop's processing of this data may constitute biometric information under certain state privacy/biometric laws. These recordings are used for evaluating your qualifications for the role and to ensure the integrity of the hiring process, including fraud prevention and as otherwise described in Section 3 (Why We Process Your Personal Data) below.
- **Background checks**: Conducted **after a job offer is made**, where required by law or applicable to the role.
- **Video, audio, and data monitoring**: If part of an assessment, some tests may include video, audio, screen activity, and data monitoring, recording, and verification to ensure fairness and prevent fraud.

We collect this information directly from you, through third-party recruiters and service providers, or from publicly available sources where relevant to your application.

3. Why We Process Your Personal Data

We process your personal data only for the purposes disclosed in this notice and for no other purpose. We process your personal data to:

- Assess your qualifications and suitability for the role.
- Communicate with you about your application and interview process.
- Verify the information you provide, including references and work eligibility.
- Conduct pre-employment assessments where applicable.
- Ensure a fair, secure, and efficient recruitment process.
- Comply with legal and regulatory obligations.
- Secure our resources, networks, premises, and assets, including to detect, prevent, investigate, and respond to suspected or alleged misconduct, use of synthetic, AI-generated or other manipulated content, violations of company policies, and fraudulent activity.
- To improve and train our artificial intelligence (AI) models used to detect, prevent, or investigate potentially fraudulent activities and/or security threats.
- Protect and defend our rights and interests and those of third parties, including to manage and respond to legal claims or disputes.

We process your personal data based on one or more of the following legal grounds:

- **Legitimate interests** – We need to evaluate candidates, conduct interviews, and make hiring decisions in a way that ensures we select the best-qualified individuals.
- **Contractual necessity** – If your application is successful, some processing is necessary to prepare for an employment contract.
- **Legal obligations** – Certain processing activities, such as verifying work eligibility, are required by law.

4. How We Share Your Personal Data

We limit access to your personal data to those involved in the hiring process. This may include:

- **Internal teams**: Recruiters, hiring managers, and relevant team members evaluating your application.
- **Service providers**: External vendors supporting our recruitment efforts, such as background check providers, assessment platforms, and HR systems.
- **Affiliated companies**: If relevant to your hiring process, we may share data within our corporate group.

Your personal data **will not be sold** or shared with unauthorized third parties. If we engage a service provider to process data on our behalf, they are required to handle it securely and in compliance with applicable laws.

5. International Data Transfers

Because Pindrop is a global company, your personal data may be transferred outside of your home country, including to the **United States**, where our primary data storage is located. For candidates applying from the **European Union (EU) or United Kingdom (UK),** we use **Standard Contractual Clauses (SCCs)** or similar safeguards to ensure compliance with data protection laws. If you would like more details on these safeguards, you may contact us.

6. Data Retention

We retain candidate data for **up to six months** following the conclusion of the hiring process. If required by law, we may retain data for a longer period. If you are not selected for a position, we will not keep your details for future job openings unless you explicitly request that we do so. If you withdraw your application, your data will be deleted, and you will no longer be considered for the role.

7. Your Rights

Depending on your location, you may have rights over your personal data, including:

- **Right to access** – You can request a copy of the data we hold about you.
- **Right to correction** – If any of your data is incorrect, you can request that we update it.
- **Right to deletion** – You may request that we delete your data, subject to legal requirements.
- **Right to object** – If we process your data based on legitimate interests, you may object in certain circumstances.
- **Right to data portability** – If processing is based on a contract or consent, you can request a transferable copy of your data.

To exercise these rights, contact us at **privacy@pindrop.com**. We will respond in accordance with applicable laws.

8. Data Security

We implement appropriate security measures to protect your personal data from unauthorized access, loss, or misuse. However, no system is completely secure, and online data transmission carries inherent risks. We encourage you to use strong passwords and avoid sharing sensitive information over unsecure channels.

9. Updates to This Notice

We may update this notice from time to time. If changes are significant, we will notify you in advance where required. Otherwise, we encourage you to check back periodically to stay informed.
For any questions, please contact **privacy@pindrop.com**.

10. Additional Privacy Information for California Residents

This section of the notice provides additional information for California and is intended to satisfy our notice and privacy policy requirements under the California Consumer Privacy Act and related regulations as amended (collectively, the "**CCPA**"). This section applies to "personal information" as defined in the CCPA, whether collected online or offline. This section does not ~~address or~~ apply to our handling of publicly available information or personal information that is otherwise exempt under the CCPA.

Categories of Personal Information Collected and Disclosed. The table below generally identifies the categories of personal information that we may collect and may have collected in the prior twelve (12) months, as well as the categories of third parties to whom we may disclose this information for a business or commercial purpose. In some cases (such as where required by law), we may ask for your consent or give you certain choices prior to collecting or using certain personal information.

Categories of Personal Information Collected	Third Party Disclosures for Business or Commercial Purposes
Identifiers. Such as name, alias, or unique personal identifier; email address, phone number, address and other personal contact details; IP address and other online identifiers.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms

	• IT administrators • Others as required by law
Categories of Personal Information Described in Cal. Civ. Code § 1798.80. Such as records containing personal information, such as name, signature, photo, contact information, education and employment history, or certain government identifiers.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law
Internet or Other Electronic Network Activity Information. Including, but not limited to, browsing history, search history, and information regarding your interaction with an internet website or application, as well as physical and network access logs and other network activity information related to your use of any company device, network, or other information resource.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • IT administrators • Others as required by law
Biometric Information. Such as physiological, biological, or behavioral characteristics that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity,	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law
Location Data. Includes general location information about a particular individual or device.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • IT administrators • Others as required by law
Characteristics of Protected Classifications Under California and Federal Law. Such as race/ethnicity, gender, sex, veteran status, disability, and other characteristics of protected classifications under California or federal law. Generally, this information is collected on a voluntary basis and is used in support of our anti-discrimination efforts, reporting obligations, or where otherwise required by law.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law
Audio, Electronic, Visual, Thermal, or Similar Information. Such as CCTV/video footage, photographs, call recordings, and other video and audio recordings (e.g., recorded meetings or interviews), as well as screen activity and other recordable data. These recordings are used solely for evaluating your qualifications for the role and to ensure the integrity of the hiring process, including fraud prevention.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law
Professional or Employment-Related Information. Such as performance information, professional membership records, references, assessment records, resumes, cover letters and work history, attendance records, conduct information (including disciplinary and grievance records), and termination data.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law
Education Information. Such as degrees earned, educational institutions attended, transcripts, training records, and other information about your educational history or background that is not publicly available personally identifiable information as defined under the Family Educational Rights and Privacy Act.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law

Inferences. Such as inferences drawn from any of the information identified above to create a profile about an individual regarding her or his preferences, characteristics, predispositions, behaviors, and personality tests and profiles reflecting skill and aptitude, including through the use of our skills assessment tests.	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law
Sensitive Personal Information. Such as certain government identifiers, racial/ethnic origin or sexual orientation (e.g., on a voluntary basis to support of our anti-discrimination efforts, reporting obligations, or where otherwise required by law), immigration or citizenship information, and health information (e.g., as necessary to provide reasonable accommodations).	• Advisors and agents • Affiliates and subsidiaries • Internet service providers, operating systems, and platforms • Others as required by law

We may also disclose the categories of personal information identified in the table above to vendors and service providers who provide services or perform functions on our behalf, as described in this notice.

Sales and Sharing of Personal Information. California privacy laws define a "sale" as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration, and "sharing" broadly includes disclosing or making available personal information to a third party for purposes of cross-context behavioral advertising. We do not sell or share (as defined by the CCPA) personal information or sensitive personal information related to candidates, including those we know who are under sixteen (16) years of age.

Sources of Personal Information. As described in Section 2 above, in general, we may collect the personal information identified in the table above from the following categories of sources:

- Directly from you
- Through third-party recruiters and recruiting platforms
- Though third-party service providers (e.g. background screeners, skills assessors, etc.)
- From publicly available sources
- From referrals and references
- From affiliates and subsidiaries

Retention of Personal Information. As described in Section 6 above, we retain candidate data for **up to six months** following the conclusion of the hiring process. If required by law, we may retain data for a longer period. If you are not selected for a position, we will not keep your details for future job openings unless you explicitly request that we do so. If you withdraw your application, your data will be deleted, and you will no longer be considered for the role.

Purposes for Collecting, Using, and Disclosing Personal Information. As described in Section 3 above, we process your personal information only for the purposes disclosed in this notice and for no other purpose:

- Assess your qualifications and suitability for the role (i.e., to evaluate candidates, conduct interviews, and make hiring decisions in a way that ensures we select the best-qualified individuals).
- Communicate with you about your application and interview process.
- Verify the information you provide, including references and work eligibility.
- Conduct pre-employment assessments where applicable.
- Ensure a fair, secure, and efficient recruitment process.
- If your application is successful, some processing is necessary to prepare for an employment contract.
- Secure our resources, networks, premises, and assets, including to detect, prevent, investigate, and respond to suspected or alleged misconduct, violations of company policies, and fraudulent activity.
- Protect and defend our rights and interests and those of third parties, including to manage and respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, or the rights, interests, health or safety of others, including in the context of anticipated or actual litigation with third parties.
- To improve and train our artificial intelligence (AI) models used to detect, prevent, or investigate potentially fraudulent activities and/or security threats.

- Comply with legal and regulatory obligations.

Sensitive Personal Information. Notwithstanding the purposes described above, we do not collect, use or disclose of sensitive personal information about candidates beyond the purposes authorized by the CCPA. Accordingly, we only use and disclose sensitive personal information about candidates as reasonably necessary and proportionate: (i) to perform our services requested by you; (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents; (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct; (iv) to verify or maintain the quality and safety of our services; (v) for compliance with our legal obligations; (vi) to our service providers who perform services on our behalf; and (vii) for purposes other than inferring characteristics about you.

Your CCPA Rights. California candidates have certain rights under the CCPA with respect to their personal information, subject to certain limitations and exceptions:

- **Know/Access**. The right to know what personal information we have collected about them, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom we disclose personal information, and the specific pieces of personal information we have collected about them.
- **Deletion**. The right to request deletion of their personal information that we have collected from them.
- **Correction**. The right to request correction of inaccurate personal information we maintain about them.
- **Opt-Out of Sales and Sharing**. The right to opt-out of the sale and sharing of their personal information. However, as discussed above we do not sell or share candidate personal information.
- **Limit Use and Disclosure**. The right to request to limit certain uses and disclosures of sensitive personal information. However, as discussed above, we do not use or disclose candidate personal information beyond the purpose authorized by the CCPA.
- **Non-Discrimination**. The right not to be subject to discriminatory treatment for exercising their rights under the CCPA.

Submitting CCPA Requests. Candidates may submit a request to us to exercise their CCPA rights to know/access, limit, delete, and to correct their personal information held by us by submitting a privacy request to us online through our webform located at https://www.pindrop.com/privacy/submit-a-request/ or via an email to privacy@pindrop.com.

We will take steps to verify your request by matching the information provided by you with the information we have in our records. Your request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative (i.e., by completing all required fields on our webform if you choose to submit a request in that manner).
- Describe your request with sufficient details that allows us to properly understand, evaluate, and respond to it.

In some cases, we may request additional information in order to verify your request or where necessary to process your request. Authorized agents may initiate a request on behalf of another individual through one of the above methods; authorized agents will be required to provide proof of their authorization, and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.