

IPM Applicant Privacy Notice

For: Job applicants and candidates who are California residents

Last Updated: August 2026

This Applicant Privacy Notice (this "Notice") describes the categories of Personal Information that Integrated Project Management Company, Inc. (the "Company," "we," "us," or "our") collects about job applicants and candidates ("Applicants," "you," or "your"), together with the sources of that Personal Information, the purposes for which we use and disclose it, and the rights available to under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA/CPRA").

1. Key Terms

"Personal Information" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

"Sensitive Personal Information" means Personal Information described in Cal. Civ. Code § 1798.140(ae), including Social Security number, driver's license or state identification card numbers, passport numbers, account log-in credentials and financial account information, precise geolocation, racial or ethnic origin, religious beliefs, union membership, contents of a consumer's mail, email, and text messages, genetic data, biometric information used for identification, information concerning health, sex life, or sexual orientation, and citizenship or immigration status.

2. Personal Information We Collect

In the preceding 12 months, we have collected the following categories and specific types of Personal Information from or about Applicants:

Category of Personal Information	Specific Types Collected
Identifiers (real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, SSN, driver's license, passport number)	Legal name, preferred name, home address, personal email address, phone number, applicant ID assigned by our applicant tracking system, LinkedIn or professional profile URLs, and — where required for background check or right-to-work verification — Social Security number, driver's license or state ID number, and passport number.
Personal information categories in Cal. Civ. Code § 1798.80(e) (name, signature, address, telephone number, employment history, education)	Signature on offer letters and pre-employment forms; prior employment history; education history; professional licenses, credentials, and certifications; and references.

Category of Personal Information	Specific Types Collected
Characteristics of protected classifications under California or federal law (voluntarily disclosed)	Voluntarily self-identified race/ethnicity, sex/gender, veteran status, and disability status collected on a voluntary basis for EEO-1 and affirmative-action purposes, and information you choose to disclose to request an accommodation for the interview or hiring process.
Commercial information	Not generally collected from applicants.
Biometric Information	Not collected from applicants. IPM does not create or store voiceprints, faceprints, or other biometric identifiers about applicants. Where the interview is conducted through Microsoft Teams and involves recording or transcription, Teams may generate labels such as "Speaker 1/Speaker 2" or attribute speech to the applicant's meeting-account name, but IPM does not extract or retain any biometric identifier template about the applicant.
Internet or other electronic network activity information	Interactions with our careers pages, applicant tracking system, and application forms; IP address; browser type; device type; and referral source.
Geolocation data	Approximate location derived from IP address. IPM does not collect precise geolocation from applicants.
Audio, electronic, visual, thermal, olfactory, or similar information	Audio and video recordings of interviews conducted through Microsoft Teams or similar platforms, together with AI-generated transcripts, meeting notes, and interviewer notes, where applicant consent has been obtained prior to recording.
Professional or employment-related information	Résumé/CV, cover letter, work samples, salary expectations, work authorization, references, prior compensation (where disclosure is not restricted by law), and information provided during interviews or assessments.
Education information (non-public, as defined in FERPA)	Degrees, transcripts, and other educational records you provide.

Category of Personal Information	Specific Types Collected
Inferences drawn from the above	Assessments and evaluations of your qualifications, experience, and fit for a role, generated by human interviewers based on the information collected.

3. Interview Recording and Transcription

The Company may record video interviews conducted through Microsoft Teams (or similar platforms) and generate an AI transcript of the interview to assist the interview panel and hiring team in accurately capturing what was discussed. Where we intend to record an interview, we will:

- Provide you with advance written notice that the interview will be recorded and transcribed;
- Obtain your affirmative consent before starting the recording, both in writing and verbally at the start of the interview;
- Confirm your right to decline recording without adverse consequence to your candidacy;
- Limit access to the recording and transcript to those with a need to know for interview evaluation and hiring decision-making;
- Retain the recording and transcript only for so long as necessary for hiring evaluation, compliance with recordkeeping obligations, and defense of legal claims.

No Biometric Information Collected. IPM does not extract or store voiceprints, faceprints, or other biometric identifier templates from Applicants. The AI transcription used in Applicant interviews is used solely to convert spoken words into text and to assist with meeting notetaking. The recording and transcript are considered "Audio, electronic, visual, thermal, olfactory, or similar information" under the CCPA/CPRA (ordinary Personal Information), not "Biometric Information" or Sensitive Personal Information used to uniquely identify you.

4. Sources of Personal Information

We collect Personal Information from the following categories of sources:

- Directly from you (e.g., your application, résumé, cover letter, interview responses, assessments, correspondence with us);
- From references and prior employers you identify;
- From third-party service providers (e.g., background-check providers, professional-reference providers, applicant tracking system providers, recruiting platforms, and Microsoft Corporation as our productivity and collaboration provider);
- From publicly accessible sources (e.g., professional social networking sites such as LinkedIn, licensing bodies);
- From recruiters and staffing agencies who refer you to us;
- From our IT systems (e.g., logs of your interactions with our careers site and applicant tracking system).

5. Purposes for Which We Use Personal Information

We use Applicant Personal Information for the following business and commercial purposes:

- To recruit, evaluate, and select candidates for open positions at the Company;
- To communicate with you about your application and possible future opportunities;
- To conduct interviews, assessments, and reference and background checks;
- To evaluate your qualifications, skills, and fit for the role;
- To make and document hiring decisions;
- To administer and improve our recruiting processes and applicant tracking systems;
- To comply with the Company's legal, regulatory, immigration, tax, EEO/affirmative-action, and reporting obligations;
- To defend or enforce the Company's legal rights and to respond to legal process;
- To provide accommodations for the interview and hiring process where requested;
- For internal quality assurance, and short-term transient use consistent with your reasonable expectations.

6. Disclosure of Personal Information

In the preceding 12 months, we have disclosed the categories of Personal Information listed in Section 2 to the following categories of third parties for business purposes:

- Service providers and contractors, including background-check providers, applicant tracking system providers, recruiting platforms, HR consultants, and productivity/collaboration providers (including Microsoft Corporation);
- Government authorities and regulators, as required by law;

We do not sell Applicant Personal Information for monetary consideration, and we do not share Applicant Personal Information for cross-context behavioral advertising.

7. Your Rights Under the CCPA/CPRA

As a California-resident Applicant, you have the following rights, subject to certain exceptions:

- **Right to Know.** Request disclosure of the categories and specific pieces of Personal Information we have collected about you, the categories of sources, the business or commercial purposes for collecting, and the categories of third parties with whom we disclose Personal Information.
- **Right to Delete.** Request that we delete Personal Information we have collected from you, subject to statutory exceptions (including recordkeeping, legal-compliance, security, and litigation-hold obligations).
- **Right to Correct.** Request that we correct inaccurate Personal Information about you.
- **Right to Portability.** Request a copy of Personal Information you have provided to us in a portable and, if technically feasible, readily usable format.

- **Right to Opt Out of Sale/Sharing.** The Company does not sell Personal Information for monetary consideration or share it for cross-context behavioral advertising, so there is no "sale" or "share" to opt out of.
- **Right to Limit Use of Sensitive Personal Information.** Request that we limit the use and disclosure of your Sensitive Personal Information to the uses that are necessary to perform the services reasonably expected in the recruiting and hiring context and to the other purposes permitted by the CCPA/CPRA regulations.
- **Right to Non-Retaliation.** You have the right not to receive retaliation or adverse hiring decisions for exercising your rights under the CCPA/CPRA, including for declining to consent to interview recording or for requesting deletion of your Personal Information (subject to our need to retain information for legal defense).

8. How to Exercise Your Rights

To exercise any of your CCPA/CPRA rights, please contact us at privacy@ipmcinc.com or call us at (630) 789-8600. You may also submit a request in writing to the mailing address in Section 11.

We will need to verify your identity before responding to a request. Verification may require you to provide sufficient information to confirm that you are the person about whom we collected Personal Information, or an authorized agent acting on that person's behalf. We will respond to a verified request within 45 days, subject to a permitted extension of an additional 45 days. You may make a data-access or data-portability disclosure request no more than twice in any 12-month period.

9. How Long We Retain Personal Information

We retain Applicant Personal Information for as long as necessary to fulfill the purposes for which it was collected and to comply with applicable legal, regulatory, and recordkeeping requirements. In general, we retain Applicant records for four (4) years or longer after the date of the application or the date the personnel action was taken, in accordance with California Government Code § 12946 (FEHA recordkeeping) and other applicable laws. Interview recordings and transcripts are retained only for the shorter of the active hiring process or ninety (90) days after the hiring decision, unless a longer retention period is required by legal-hold, contractual, or regulatory obligations. Detailed retention periods are set forth in the Company's Records Retention Schedule, which is available on request.

10. Contact Information

Mail: Integrated Project Management Company, Inc., Attn: Legal Department, 60 N. Frontage Road, Suite 300, Burr Ridge, IL 60527

Phone: (630) 789-8600

Email: privacy@ipmcinc.com

11. Changes to This Notice

We may update this Notice from time to time. We will post the updated version at the location referenced in the general Privacy Policy and update the "Last Updated" date above. Material changes will be communicated to Applicants where practicable.