Pantheon Systems, Inc.
Applicant Privacy Policy

Last Updated October 2026

This Privacy Policy ("Privacy Policy") addresses how Pantheon Systems, Inc. and its group companies, including Pantheon Platform UK Limited and Pantheon Platform Ireland Limited, and Pantheon Platform International, Inc. are committed to protecting your personal data. This Privacy Policy applies to each group company. References to "Pantheon", "we", "us" or "our" are to the relevant group entity that is responsible for processing your personal data. The Pantheon group entity to which you apply (the prospective employing entity) is the primary data controller responsible for your personal data. Specifically: for applicants for roles in the United Kingdom, the data controller is Pantheon Platform UK Limited; for applicants for roles in the European Economic Area and Switzerland, the data controller is Pantheon Platform Ireland Limited; for applicants for roles in the United States and Canada, the data controller is Pantheon Systems, Inc. Pantheon Platform Canada, inc.; for applicants for roles in the Philippines, the data controller is Pantheon Systems PH,Inc.; and for applicants for roles in India, the data controller is Pantheon Platform India Private Limited.

This Privacy Policy applies to the processing of personal data of individuals who apply to work for us in the UK, EEA, Switzerland, United States, Canada, the Philippines and India and describes the types of personal data we may collect. It also explains how we use AI-assisted tools in our recruitment process. Additional information for applicants in specific countries is in the Supplements at the end of this Privacy Policy. If a Supplement conflicts with the rest of this Privacy Policy for your location, the Supplement applies. If your application is successful, the processing of your personal data as a member of staff will be governed by our Employee Privacy Policy for the U.K., EEA and Switzerland, available at https://legal.pantheon.io. We also have a separate privacy policy that applies to the processing of personal data of visitors to our website and users of our services, our Privacy Policy for the U.K., EEA and Switzerland, available at https://legal.pantheon.io/.

It is important that you read this Privacy Policy together with any other privacy policy or fair data processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are aware of how and why we use your information.

Questions regarding this Privacy Policy should be emailed to privacy@pantheon.io or mailed to Legal/Privacy, Pantheon Systems, Inc., 717 California Street, Floor 2, San Francisco, California 94108. You may also call Pantheon at +1-855-927-9387 and ask for the General Counsel.

How we Collect and Use your Data

Information Gathered

Personal data means any information about an individual from which that person can be identified. It does not include anonymised data.

In connection with your application for work with us, we will collect, store and use the following categories of personal information about you:

- The information you have provided to us in your Resume/ CV and covering letter.

- The information you have provided on our application form, including name, location (City), telephone number, personal email address, education history, qualifications and employment history.
- Any information you provide to us during the interview process.
- The results of any tests, assessments or work samples you complete as part of the application process.
- Information obtained from sources other than yourself referred to below.
- Information generated by the tools we use in the recruitment process, including Talent Matching output (match scores and explanations), and interview recordings, transcripts and AI-generated notes and summaries (if you agree to recording).
- If you choose to verify your identity with CLEAR: whether the check was passed, and limited details from it (your name, email address, phone number and IP address). We do not receive your ID image, selfie or biometric data.
- Technical information, such as IP address and device data, used to detect fraudulent or automated applications.

This may involve us collecting, storing and using the following types of more sensitive personal information:

- Information about your race or ethnicity, religious or philosophical beliefs, sexual orientation.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

Sources

We collect personal information about applicants from the following sources:

- You, the applicant.
- Approved recruitment agencies, from which we collect the following categories of data: name, location (City), telephone number, personal email address, education history, qualifications and employment history.
- Hire Right, our approved background check provider, from which we collect the following categories of data (only where permitted by, and conducted in accordance with, the law applicable in your jurisdiction, and where proportionate to the role for which you have applied):

  Criminal record search results

  Right to work

  Education records

- CLEAR, our identity verification provider, from which we receive (through Greenhouse) whether your identity check was passed and limited details: your name, email address, phone number and IP address.

- Your named referees, from whom we collect the following categories of data:

  Confirmation of prior working relationship, duration of working relationship, assessment of interpersonal skills and other relevant attributes.

- Publicly accessible sources, such as professional networking sites (for example, LinkedIn) and professional registers, from which we may collect employment history and qualifications. If you do not provide information when requested which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application successfully.

Legal Basis for Processing Personal Data

We only process your personal data where applicable law permits or requires it, including where the processing is necessary in order to take steps, at your request, prior to entering into an employment contract or other engagement with you, where the processing is necessary to comply with a legal obligation that applies to us, for our legitimate interests or the legitimate interests of third parties (where your interests and fundamental rights do not override those interests), to protect your vital interests, or with your consent if applicable law requires consent. We process your personal data for the purposes of administering our recruitment process, including the following:

- assessing your skills, qualifications and suitability for the role for which you have applied;
- complying with applicable law;
- verifying the information provided by you or by third parties, including carrying out reference checks and, where permitted by and conducted in accordance with applicable local law and proportionate to the role, background checks;
- communicating with you about your application and the recruitment process;
- making informed hiring decisions and, if your application is successful, taking steps to enter into a contract with you;
- keeping records relating to our hiring processes and reviewing and improving those processes; and
- responding to and defending against legal claims (for example, claims of discrimination in the recruitment process).

We will only process your personal data for the purposes for which we collected it, or for compatible purposes. If we need to process your personal data for an incompatible purpose, we will provide notice to you and, if required by law, seek your consent. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

We may also process your personal data for our own legitimate interests, including for the following purposes:

- to prevent fraud;

- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- to support internal administration with our affiliated entities;
- to conduct data analytics to review, understand and improve our recruitment processes.
- As explained in "How we use AI-assisted tools in recruitment" below, we do not make recruitment decisions based solely on automated processing (including profiling) which produce legal or similarly significant effects concerning you. If this changes, we will notify you in advance and you will have the rights described in this Privacy Policy.

How we use AI-assisted tools in recruitment

We use tools provided by our applicant tracking system provider, Greenhouse Software, Inc. ("Greenhouse"), and its partners, to support our recruitment process. Greenhouse processes your personal data on our behalf under a written contract. The tools are:

- **Talent Matching (AI-assisted application review).** Talent Matching compares your resume and responses to application questions against the job requirements our recruiters set for the role, and the weight they give each, and produces match categories with explanations. Our recruiters and hiring managers review all Talent Matching output and make every decision about your application. Talent Matching does not automatically advance, reject or disqualify any candidate or make hiring decisions, and it does not infer emotions or sentiment. In the UK, EEA and Switzerland we rely on our legitimate interests in assessing applications consistently and efficiently. You can ask for a manual review without Talent Matching: see "Your choices to control your data" below.
- **Greenhouse Notetaker (AI interview notes).** Only if you agree in advance, Notetaker records and transcribes your interview and produces AI-generated notes and a summary for our interviewers. A visibly labelled Notetaker joins the call. Greenhouse's sub-processors Recall.ai (recording and transcription, on servers in the United States) and OpenAI (AI summaries) process the interview. Agreeing is optional and your decision will not be held against you. If you withdraw before the interview, Notetaker will not join; if you withdraw during the interview, tell the interviewer, who will remove it. Recordings are deleted after 30 days. Transcripts, notes and summaries are kept with your application record. Interviewers can see their own interview materials, and hiring team members and administrators with the relevant permission can see others'. Notetaker does not analyse your emotions or personality.
- **Identity verification with CLEAR.** At the offer stage we ask you to verify your identity using CLEAR, an independent identity verification provider. You give your government-issued ID, a selfie and related details directly to CLEAR, which checks them, including a facial (biometric) match. CLEAR is the controller of that information and handles it under its own privacy notice, which CLEAR shows you, with its data-sharing approval screen, when you start the check: CLEAR Privacy Policy. We do not receive or store your ID image, selfie or biometric data. Greenhouse tells us whether the check was passed and gives us limited details (your name, email address, phone number and IP address). To have the information CLEAR holds deleted, contact CLEAR directly. A failed or incomplete check does not automatically reject you or block an offer: a person reviews it and you can explain.

If you prefer not to use CLEAR, tell us and we will verify your identity another way, for example in person or by live video call. Your choice will not be held against you.

- Fraud and spam checks. Greenhouse may analyse technical signals, such as IP address and device information, to detect fraudulent or automated applications.

We do not use these tools to make solely automated decisions about you. Greenhouse and its partners do not use your personal data to train AI models for other customers. Greenhouse has Talent Matching independently audited for bias by Warden AI and publishes its bias audit statement at https://www.greenhouse.com/bias-audit-statement. You can ask for an alternative evaluation, ask how a tool was used in your case, and ask a person to review any decision: see "Your choices to control your data" below.

Collection and Use of Special Categories of Personal Data

The following special categories of personal data are considered sensitive under UK and EU law and may receive special protection:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- data concerning health;
- data concerning sex life or sexual orientation.
- Data relating to criminal convictions and offences may also receive special protection under UK and EU law.

We may collect and process the following special categories of personal data, where you voluntarily provide them or where we are otherwise permitted or required to process them by law, in order to carry out our obligations and exercise our rights in connection with the recruitment process, or as applicable law otherwise permits:

- physical or mental health information or disability status, to consider whether we need to make reasonable adjustments to the recruitment process (for example, during assessments or interviews) and to comply with our legal obligations.
- race or ethnic origin, religious affiliation, health information and sexual orientation to ensure meaningful equal opportunity monitoring and reporting. Providing this information is entirely voluntary, your answers (or your decision not to answer) will have no bearing on your application, and the information is kept separate from the selection process and analysed on an aggregated and, where possible, anonymised basis.

Where we have a legitimate need to process special categories of personal data for purposes not identified above, we will only do so after providing you with notice and, if required by law, obtaining your prior, express consent. Where required under UK law, we process special category data and criminal offence data (including the results of any background checks) in accordance with our appropriate policy document.

We will always treat special categories of personal data as confidential, and we will only share such data internally where there is a specific and legitimate purpose for sharing the data. As set out below, we have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

We will only retain special categories of personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes.

How we share and manage your data

Sharing of Information

We will only disclose your personal data to third parties where required by law or to our employees, contractors, designated agents, or third-party service providers who require such information to assist us with administering the recruitment process. Third-party service providers may include, but are not limited to, recruitment platform and applicant tracking system providers (including Greenhouse), interview recording and transcription tools, identity verification providers (including CLEAR), background check providers, and data storage or hosting providers. These third-party service providers may be located outside of the country where you apply, including in the United States. Greenhouse uses sub-processors, including Recall.ai (interview recording and transcription) and OpenAI (AI-generated interview summaries). Greenhouse's current list of sub-processors is at https://www.greenhouse.com/subprocessors-in-use.

We require all our third-party service providers, by written contract, to implement appropriate security measures to protect your personal data consistent with our policies and any data security obligations applicable to us. We do not permit our third-party service providers who process your personal data on our behalf to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes in accordance with our instructions.

We may also disclose your personal data for the following additional purposes, where permitted or required by applicable law:

- to other members of our group of companies (including outside of the UK, EEA and Switzerland) for the purposes set out in this Privacy Policy and as necessary to administer the recruitment process;
- as part of our regular reporting activities to other members of our group of companies;
- to comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders; when we disclose your personal data to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal data necessary for the specific purpose and circumstances;
- to protect the rights and property of Pantheon;
- during emergency situations or where necessary to protect the safety of persons;
- where the personal data is publicly available;
- if a business transfer or change in ownership occurs and the disclosure is necessary to complete the transaction; in these circumstances, we will limit data sharing to what is absolutely necessary, and we will anonymise the data where possible;
- for additional purposes with your consent where such consent is required by law.

Security

Pantheon uses appropriate administrative, technical, organizational, and physical security measures to protect your personal data against accidental or unlawful destruction, loss, and alteration, and against unauthorised disclosure and access. We use standard industry practices to protect personal information, including firewalls, SSL encryption, system redundancies, and co-location in a 24/7 secured, controlled environment.

Data Transfers

Your personal data may be transferred to, and processed in, countries other than the country in which you reside. Specifically, Pantheon's data is hosted on servers located around the world, including in the United States of America, the United Kingdom, the EEA, and elsewhere. Our group companies and third party service providers and partners may operate around the world. This means that when Pantheon collects your personal data, such information may be processed in any of these countries or elsewhere. Whenever we transfer your personal data outside of the UK, EEA, or Switzerland as the case may be, we ensure that a similar degree of protection is afforded to it by having at least one of the following safeguards in place: (i) the country to which we transfer your personal data has been deemed to provide an adequate level of protection for personal data, or (ii) we have in place specific contracts approved by the UK, EEA, and Switzerland (i.e., EU SCCs, UK IDTA/Addendum and Swiss clauses). Greenhouse, our applicant tracking system provider, relies on the EU-U.S. Data Privacy Framework and the UK Extension to it where it is certified, with standard contractual clauses as a secondary mechanism. Greenhouse's interview recording provider, Recall.ai, processes interview recordings on servers in the United States, and Greenhouse's agreements with Recall.ai and OpenAI use standard contractual clauses. Transfers of personal data from Canada, the Philippines and India are described in the relevant Supplement. For more information about how we transfer your information, please contact privacy@pantheon.io.

Pantheon Systems, Inc. and Pantheon Platform International, Inc. ("Pantheon US") comply with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the U.S. Department of Commerce. Pantheon Systems, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("EU-U.S. DPF Principles") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Pantheon Systems, Inc. has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles ("Swiss-U.S. DPF Principles") with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. Pantheon's U.S. subsidiary, Pantheon Platform International, Inc., is also certified under these frameworks and is bound by the same obligations and principles. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework ("DPF") program, please visit https://www.dataprivacyframework.gov/ and you can view the certification for Pantheon US at https://www.dataprivacyframework.gov/list.

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Pantheon US commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to TRUSTe, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://feedback-form.truste.com/watchdog/request for more information or to file a complaint. The services of TRUSTe are provided at no cost to you. Under certain conditions, you may invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms.

You may direct inquiries or complaints concerning Pantheon US's processing of personal information to privacy@pantheon.io. Pantheon will respond within one month. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. Pantheon US is subject to the investigatory and enforcement powers of the Federal Trade

Commission (“FTC”). The FTC has jurisdiction over Pantheon US’s compliance with the EU-US DPF and the UK Extension to the EU-US DPF, and the Swiss-US Data Privacy Framework (“Swiss-US DPF”).

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Pantheon US commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities and the UK Information Commissioner’s Office (“ICO”) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship.

In the context of an onward transfer, Pantheon US is responsible for the processing of personal data it receives under the DPF Principles and subsequently transfers to a third party acting as an agent on our behalf. Pantheon US will remain liable under the DPF Principles if our agent processes your personal data in a manner inconsistent with the DPF Principles.

Your choices to control your data

Accessing, Updating, Correcting, Erasing and Objecting to the Use of Information

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during the recruitment process. By law you may have the right to request access to, correct, and erase the personal data that we hold about you, or object to the processing of your personal data under certain circumstances. You also have the right not to be subject to a decision based solely on automated processing which produces legal or similarly significant effects concerning you. You can ask us to review your application manually, without Talent Matching, for any job you apply for. If you do, Talent Matching will not evaluate your application and any match score and reasoning already generated for it will be deleted. You can also ask us to explain how an AI-assisted tool was used in relation to your application, and ask for a person to review any decision you disagree with. We will tell you the outcome of any review in writing. You may also have the right to request that we transfer your personal data to another party. If you want to review, verify, correct, or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact us at privacy@pantheon.io. You do not need to use particular words or a particular channel, although using the contact details below helps us respond faster.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal data that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our Record Retention Policy and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Where you have provided your consent to the collection, processing, or transfer of your personal data, you may have the legal right to withdraw your consent under certain circumstances. To withdraw your consent, if applicable, contact us at privacy@pantheon.io. Declining or withdrawing your consent (for example, to interview recording) will not be held against you. Withdrawal does not affect processing already carried out.

Contact Details to Exercise a Right, Ask a Question, or Submit a Complaint

If you wish to exercise any of the rights above, click **here** or please contact us privacy@pantheon.io or mail a request to Legal/Privacy, Pantheon Systems, Inc., 717 California Street, Floor 2, San Francisco, California 94108. You may also call Pantheon at +1-855-927-9387 and ask for the General Counsel.

You will not have to pay a fee to access your personal data or exercise the above rights, except that we may charge a fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request. We may need specific information from you to confirm your identity and ensure your right to access your personal data or exercise any of your rights. This is a security measure to ensure that your personal data is not disclosed to a person who does not have a right to receive it. We endeavor to respond to all requests within one month; however, occasionally, it could take longer if your request is complex or you have made a number of requests. If this occurs, we will notify you and update you on the status of your request. We will not retaliate against you, or treat you less favourably, for exercising any of your rights or making any request described in this Privacy Policy.

You may direct inquiries or complaints concerning Pantheon's processing of personal information to privacy@pantheon.io. Pantheon will respond within the time prescribed by applicable law and, if applicable law does not address such time frame, within one month.

You have the right to contact the ICO (UK), the Data Protection Commission (Ireland), the Federal Data Protection and Information Commissioner (Switzerland, available at https://www.edoeb.admin.ch) or the data protection authority in your jurisdiction. We would, however, appreciate the chance to address your concerns before you approach a data protection authority, so please contact us in the first instance through one of the methodologies noted, above. Contact details for the ICO are available at www.ico.org.uk, contact details for the Data Protection Commission are available at https://www.dataprotection.ie/en and contact details for data protection authorities in the European Economic Area are available here European Data Protection Board - Members.

Receive Notice of Changes

We reserve the right to update this Privacy Policy at any time, and we will provide you with a new Privacy Policy when we make any updates. If we would like to use your previously collected personal data for different purposes than those we notified to you at the time of collection, we will provide you with notice and, where required by law, seek your consent, before using your personal data for a new or unrelated purpose. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

Record Retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal data, we consider applicable legal requirements, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes we process your personal data for, and whether we can achieve those purposes through other means. If you are successful in your application to join Pantheon, we will retain the personal data obtained during the recruitment process as part of your employment record, in accordance with our Employee Privacy Policy and our Record Retention Policy, for a period of 7 years following the termination of your employment. If you are unsuccessful, or opt not to join us, we will retain your personal data for a period of 1 year following the date that a decision is made, after which it will be securely deleted, unless you have consented to us retaining your details to consider you for future opportunities. Interview recordings made with Greenhouse Notetaker are deleted after 30 days. Transcripts, AI-generated notes, Talent Matching output and the result of any identity verification check are kept with your application record for the periods above. CLEAR keeps the ID image, selfie and related identity data it collects under its own policies, and you must ask CLEAR directly to delete them. Greenhouse keeps job calibration settings and system logs under its own retention policies. Longer or shorter periods apply in some countries: see the Supplements. We may keep records for longer where we need them to establish, exercise or defend legal claims, or where the law requires.

Under some circumstances we may anonymise your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. Once the recruitment process has concluded, we will retain and securely destroy your personal data in accordance with the retention periods set out above, our Record Retention Policy and applicable laws and regulations.

Supplements for specific countries

These Supplements add to the rest of this Privacy Policy for applicants in the countries below. The UK, EEA and Switzerland are covered by the main text.

United States

California applicants (notice at collection)

This section applies to California residents and is our notice at collection under the California Consumer Privacy Act (CCPA).

- **What we collect.** Identifiers and contact details; professional and employment information; education information; audio recordings and transcripts of interviews (with your agreement); inferences from Talent Matching about how your qualifications match the role; the result of any CLEAR identity check and limited details from it; internet and device information used to detect fraudulent applications; and sensitive personal information you choose to give us, such as race or ethnic origin, health or disability, and sexual orientation. If you verify your identity with CLEAR, CLEAR collects biometric information directly; we do not receive it.
- **Why.** For the purposes described in "Legal Basis for Processing Personal Data" above.
- **Sale and sharing.** We do not sell your applicant personal information or share it for cross-context behavioural advertising. We use sensitive personal information only for purposes the CCPA permits, and not to infer characteristics about you.
- **How long we keep it.** For unsuccessful applicants, we keep application records, including data created by automated tools, for 12 months from the date the record was made or the hiring decision, whichever is later. Interview recordings are deleted after 30 days. Application records for successful applicants will be retained in accordance with our Employee Privacy Policy which is available upon request to privacy@pantheon.io.
- **Your rights.** You can ask us to tell you what personal information we hold and how we use it, to delete it, or to correct it, and we will not treat you less favourably for doing so. To make a request, use the web form or email privacy@pantheon.io, or call +1-855-927-9387. We will confirm receipt within 10 business days and respond within 45 days (we may extend this once by up to 45 more days and will tell you if we do). We may need to verify your identity. You can use an authorised agent.
- **Automated tools.** Talent Matching assists our recruiters; it does not replace them. [If we later use automated decision-making technology to make or substantially replace significant decisions about applicants, we will give you the notice and rights California law requires before we do.]

Background checks

Where we use HireRight, a consumer reporting agency, for background checks, we will give you a separate disclosure and obtain your written authorisation first, and we will tell you before taking any action based on a report, as the Fair Credit Reporting Act and state laws require.

Illinois

If you apply for a role in Illinois: we tell you when we use AI in recruitment (see above). We obtain your consent before an interview is recorded or analysed by AI. If you verify your identity with CLEAR, CLEAR (not Pantheon) collects and holds your biometric information (a facial match) and handles it under its own notice and retention policy. We do not receive or store it.

New York City

If you live in New York City, we use Greenhouse Talent Matching, an automated employment decision tool, to help assess candidates. It compares your resume and application answers against the job requirements our recruiters set for the role and the weight they give each. We will give you at least 10 business days' notice before first using it on your application. You can ask for an alternative evaluation or an accommodation, and for information about the type and source of the data used and how long we keep it, at privacy@pantheon.io. A summary of the latest independent bias audit is at legal.pantheon.io.

Interview recording

Recording laws vary by state. We record an interview only with the consent of everyone taking part.

Canada

Privacy laws that may apply to your application include the federal Personal Information Protection and Electronic Documents Act, the Personal Information Protection Acts of Alberta and British Columbia, and Quebec's private sector privacy law.

Consent. We collect, use and disclose your personal information with your consent, which you give by applying and, where needed (for example for interview recording), separately. You can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Withdrawing may mean we cannot continue with your application.

- **Your rights.** You can ask for access to, and correction of, your personal information. Contact our Privacy Team at privacy@pantheon.io. If you are not satisfied, you can complain to the Office of the Privacy Commissioner of Canada or, where applicable, the Office of the Information and Privacy Commissioner of Alberta or British Columbia, or the Commission d'accès à l'information du Québec.
- **Transfers outside Canada.** Your personal information may be processed outside Canada, including in the United States and by Greenhouse and its sub-processors. It may be accessible to courts, law enforcement and national security authorities there. Contact us for more information about our service providers outside Canada.
- **Ontario.** If you apply for a publicly advertised role in Ontario: we use artificial intelligence (Talent Matching) to screen, assess or select applicants, and we say so in the job posting and application form.
- **Quebec.** Talent Matching uses profiling to assess how your qualifications match a role. We do not make decisions based exclusively on automated processing. If that changes, we will tell you when we communicate the decision and, on request, tell you the personal information used, the reasons and main factors, and your right to have the information corrected and the decision reviewed by a person. We do not collect or store biometric information; if you verify your identity with CLEAR, CLEAR collects it under its own notice.

Philippines

This section applies to applicants for roles in the Philippines and is given under the Data Privacy Act of 2012 (Republic Act No. 10173), its Implementing Rules and the issuances of the National Privacy Commission (NPC).

- **Basis.** We process your personal information to take steps at your request before entering into an employment contract, to comply with legal obligations, for our legitimate interests, and with your consent where required. We process sensitive personal information (including government-issued identifiers and health information) only with your consent or where the law otherwise allows.
- **Your rights.** You have the right to be informed, to object, to access, to correct, to have your data erased or blocked, to data portability, to claim compensation where you have been harmed, and to complain to the NPC. You also have the right to be informed about automated processing and profiling. Talent Matching is used to assist our recruiters, who make the decisions.
- **Data Protection Officer.** Contact our privacy team at privacy@pantheon.io.
- **Transfers.** We share your personal data with group companies and service providers outside the Philippines, including in the United States. We require them, by written agreement, to protect it to a comparable standard.
- **Complaints.** You can complain to the National Privacy Commission at https://privacy.gov.ph.

India

This section applies to applicants for roles in India. Until 13 May 2027 we handle your information in line with the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. From 13 May 2027 the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 will apply, and this section will apply in line with them.

- **Consent.** We collect sensitive personal data or information (such as health information) only with your consent, given in writing or electronically. For other personal data, we rely on your consent or another lawful ground. You can withdraw your consent at any time, as easily as you gave it. If you withdraw, we may not be able to continue with your application, and we will stop processing your data unless the law requires us to keep it.
- **Your rights.** You can ask to see a summary of the personal data we hold, ask us to correct or erase it, and ask us to resolve a grievance. You can nominate another person to exercise these rights if you die or become incapacitated.
- **Grievance Officer.** Contact our Privacy Team at privacy@pantheon.io We will respond within the period the law requires. From 13 May 2027 you can also complain to the Data Protection Board of India once you have used our grievance process.
- **Transfers.** Your personal data may be transferred to and processed outside India, including in the United States, by us, Greenhouse and its sub-processors. We will protect it to a standard the law requires.