Recruitment Privacy Statement

Effective Date: January 1, 2023

Ancestry is committed to the responsible management, use, and protection of personal information collected from its applicants and employees. This Recruitment Privacy Statement ("Privacy Statement") describes how Ancestry collects, uses, discloses, transfers, and stores personal information in our recruitment process for companies in the Ancestry group. For the purpose of this Privacy Statement, the term personal information means any data relating to an identified or identifiable person that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular living individual. This Privacy Statement applies to all candidates and individuals applying for a role with Ancestry at all times during the application and recruitment process. In alignment with the EU's General Data Protection Regulation (GDPR), the United Kingdom's GDPR, the California Consumer Privacy Act of 2018, and other applicable data privacy and data protection laws, this Privacy Statement provides details on your personal data rights and how to exercise those rights. However, the application of any particular law will depend on each individual case. In addition, we may inform you about the processing of your data separately (for example in consent forms, terms and conditions, and just-in-time notices).

If you disclose personal information to us or share data with us about other individuals, such as co-workers, supervisors or other persons looking for employment, we assume that you have obtained consent from those persons and the data you share is accurate. Please also make sure that these individuals have been informed about this Privacy Statement.

1. Who is the controller for processing your data?

A. For applicants in North America, Ancestry.com Operations, L.P. ("Ancestry.com"), with offices at 1300 West Traverse Parkway Lehi, UT 84043, USA is the data controller under this Privacy Statement, unless we tell you otherwise, for example in additional privacy notices, or on a form or in a contract. You may contact us regarding any data protection concerns and to exercise your rights under Section 7 below as follows:

Ancestry.com Operations, L.P.
Attn: Privacy Office
1300 W. Traverse Parkway
Lehi, UT 84043 USA
peopleops@ancestry.com

B. For applicants in Europe and the rest of the world, Ancestry Ireland Unlimited Company ("AIUC"), with offices at 52-55 Sir John Rogerson's Quay, Dublin D02 NA07 Ireland, is the data controller under this Privacy Statement, unless we tell you otherwise, for example in additional privacy notices, on a form or in a contract. You may contact us in regard to any data protection concerns and to exercise your rights under Section 7 below as follows:

Ancestry Ireland Unlimited Company
52-55 Sir John Rogerson's Quay
Dublin D02 NA07
Ireland
peopleops@ancestry.com

This Privacy Statement also applies where a subsidiary within the Ancestry group is the potential employer. These additional parties are joint controllers for the processing set out in this Privacy Statement. If you wish to receive information about the controllers for a specific employment opportunity, you are welcome to ask us as part of your access right set forth in Section 7 below. Either Ancestry.com or AIUC, respectively, remain your primary contact even if there are subsidiaries acting as joint controllers of your personal information.

2. The types and purposes of personal information collected by Ancestry

We will collect personal information about you in relation to your job application, specifically:

- to communicate with you about your job application and potential future job opportunities;
- to assess your skills, qualifications and your suitability for our career opportunities;
- to support and manage the job application process;
- where necessary, to comply with applicable legal or regulatory requirements;
- to deal with legal disputes and to establish, exercise and defend (potential) legal claims; and
- to report the demographic makeup of our applicants (where lawful).

Some of this personal information will have been obtained directly from you and some may be obtained from third parties. The personal information collected as part of the recruitment process will vary by location. For example, in certain jurisdictions, we are required to collect and retain certain information to comply with applicable regulations. In other jurisdictions, there is no authorization to collect such data. Likewise, certain jurisdictions do not allow for the collection of data regarding criminal offenses, convictions and/or expunged records. You can obtain more information about these requirements by contacting Ancestry as set forth in Section 1.

A. For **all** applicants, worldwide, Ancestry will collect:

Type of Data	Source	Lawful Basis / Purpose for Collection
Contact information such as name, email address, telephone numbers	Candidate	You voluntarily provide this information and consent to Ancestry processing it.
All background information contained within your letter of application and CV/resume, including but not limited to employment/salary history, educational history, professional licenses and certifications	Candidate, prior employers, and education providers	You voluntarily provide this information and consent to Ancestry processing it.
Information relating to employment references	Candidate's LinkedIn profile and information provided by prior employers	The processing is necessary for the legitimate interests pursued by Ancestry. In this instance, the legitimate interest of Ancestry is to carry out adequate checks on candidates to assess their suitability for employment.
Details of work authorisation/ authorization status	Candidate	This data is necessary to comply with a legal obligation (e.g. employers have a legal requirement to ensure employees are authorized to work within the relevant jurisdiction).
Special Category Personal Data related to information about your health, including any medical needs or conditions	Candidate and possibly health care providers	You voluntarily provide this information and consent to Ancestry processing it in connection with requests for reasonable accommodation, special working conditions or other forms of assistance.
Interview details, and outcomes of any recruiting exercises/assessment you complete	Candidate, assessment providers, interviewers	You voluntarily provide this information and consent to Ancestry processing it. The processing is necessary for the purposes of Ancestry's legitimate interest in assessing suitability for employment through interviews and/or assessments.
Registration to Ancestry's talent community/job alerts, including name, email, phone number, resume/CV, skills, career interests, IP address, devices and favorites.	Candidate	You voluntarily provide this information to access the recruiting site and consent to processing by Ancestry.
Personal data included on website profiles such as LinkedIn,GitHub, Portfolio, or other website profiles provided by candidate along with any inferences drawn from any of the information identified in this subdivision to create a profile about a candidate.	Links voluntarily provided by candidate at time of application	You may voluntarily provide this information and consent to processing by Ancestry.

B. For applicants in **North America**, Ancestry will collect:

Type of Data	Source	Purpose for Collection
Background Screening Information including, but not limited to: Social Security number, current and past addresses, current and past education and employment, criminal history, civil records, sex offender registry search	Employment history and background check details including criminal history, public records such as government agency, civil court index, and academic institution records, sex offender databases	For Ancestry to carry out adequate background checks on candidates and to assess their suitability for employment
Demographic Information including gender, racial or ethnic origin and veteran status	Voluntarily provided/disclosed by candidate	Gender, Racial or ethnic origin, and veteran status for compliance with government-required EEO reporting, diversity reporting and internal analytics of company demographics

C. For applicants in **EU and Rest of the World**, Ancestry will collect:

Type of Data	Source	Purpose for Collection
Background Screening Information including current and past education and employmen	Employment history and background check details including criminal history, public records such as government agency, civil court index, and academic institution records, sex offender databases	For Ancestry to carry out adequate background checks on candidates and to assess their suitability for employment

D. Cookies and Similar Tracking Technologies

Ancestry's careers website uses cookies and tracking technologies as described in the Settings Page of our careers website. Please refer to this page to learn about these cookies and the controls provided to you.

Cookie Name	Description	Default Expiration Time	GDPR Classification	Personal Data within Cookie?
_clinch_session	This functionality is used by the Clinch platform to maintain a candidate's session integrity, whilst they are accessing the system. It is not stored beyond the session's duration and does not store personal data.	Expires when session ends	Strictly Necessary	No
ctc_rejected	This cookie is used to record that Clinch performance cookies have not been accepted, and to stop the cookie Consent box from appearing. It is localized per candidate device -- there is no PII and no record on the back end.	Expires when session ends	Functionality/ preference	No
ctc	A cookie that identifies the candidate if they had agreed to the cookie policy. Each time a user takes an action on the career site, Clinch examines the identifier in the cookie to look up the candidate.	24 Months	Performance	A randomly assigned unique identifier that identifies the candidate to the platform.
cts_session	A cookie that ties together all the activity (page views, forms, etc.) and interactions per visitor (identified by the ctc cookie above) in one session or visit to the site.	15 minutes or when session ends	Performance	A randomly assigned unique identifier that identifies the candidate's session to the platform.

3. When Does Ancestry Disclose Your Information and Who are the Recipients?

As part of the recruitment process, Ancestry may disclose personal information in the following circumstances:

- To third-party service providers which process personal information on our behalf:
  o Investigators who conduct background checks;
  o Service providers supporting Ancestry's Career Site;
  o Service providers who process data on Ancestry's behalf, including recruiting and human resources tools;
- To contact references provided by applicants in regard to prior employment and qualifications;
- We may share your personal information if it is reasonably necessary to comply with valid legal process (e.g., subpoenas, warrants) or protect the rights, property, or safety, of Ancestry and its employees;
- If Ancestry is acquired we may share your personal information with the acquiring or receiving entity. The promises in this Privacy Statement will continue to apply to your personal information that is transferred to the new entity.

4. Data Transfer

Ancestry stores all of its data in servers located in the United States. For data transfers from the EU to the United States, which is considered to be a country without adequate statutory data protection, the transfer of data is governed by the revised European Commission's standard contractual clauses and the UK's International Data Transfer Agreement Addendum. These contractual arrangements compensate for the differences in legal protection to some extent. However, contractual precautions cannot eliminate all risks (namely of government access abroad). You should be aware of these remaining risks, even though they may be low in an individual case. You may request a copy of our data transfer agreements by emailing dpo@ancestry.com.

5. Data Retention

A. For Applicants in North America:

Your personal information will be stored in accordance with applicable laws and kept as long as needed to carry out the purposes described in this Privacy Statement or as otherwise required by applicable law.

B. For Applicants in the EU and rest of the world:

Your data will be retained for a period of one (1) year, unless you request that we delete it before that time. Retained information includes information you entered on your application, your resume, (if you provided one), interview feedback, and outcomes of any recruiting exercises/assessments you complete.

If your job application is successful, the personal information collected during the recruitment process will be added to your human resources file and governed by Ancestry's employee policies.

6. Your Data Rights

Depending on where you are located, you may have certain rights in regard to the personal data Ancestry holds about you. These may include the right to:

- Request access to your personal information;
- Withdraw your consent to the processing of your application data. Withdrawal of consent will naturally end the application process. Moreover, withdrawal of consent does not affect the lawfulness of processing based on consent prior to withdrawal;
- Correct personal information if incomplete or inaccurate;
- Delete your personal information;
- Restrict the processing of your personal information (for example, while your request for correction is being considered);
- Object to the processing of your personal information carried out on the basis of our legitimate interests;
- Receive a copy of your personal information in an electronic and machine-readable format;
- Not be subject to a decision based solely on automated decision making or profiling; and finally
- Lodge a complaint with a data protection authority about Ancestry's processing of your personal information. In the event that you wish to make a complaint about how your personal information was processed by Ancestry or in regard to how Ancestry has handled any request or objection made by you, you have the right to make a complaint to the Irish Data Protection Commission (Complaints handling, Investigations and Enforcement For Individuals | Data Protection Commissioner) or any other competent supervisory authority in the country of residence. A list of EU data protection authorities is available at: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

You can exercise your applicable rights by contacting Ancestry using the details set forth in Section 1(B).

Ancestry will not discriminate against you for exercising your rights.

In US states where residents are allowed additional individual rights, Ancestry is committed to honoring those rights for such residents, including requests that may limit how we use and share your personal information, consistent with applicable law. To submit a request based on local law, please contact us as indicated in Section 1(A). We will respond to your request consistent with applicable law, and if any circumstances cause delay in our response, you will be promptly notified.

7. Data Security

Ancestry maintains a comprehensive information security program using administrative, physical, and technical safeguards.

The specific security measures used are based on the sensitivity of the personal information collected. We have measures in place to protect against inappropriate access, loss, misuse, or alteration of personal information under our control.

Ancestry’s Information Security Team regularly reviews our security and privacy practices and enhances them as necessary to help ensure the integrity of our systems and your personal information.

We use secure server software to encrypt personal information, and we only partner with security companies that meet and commit to our security standards. While we cannot guarantee that loss, misuse or alteration of data will not occur, we use reasonable efforts to prevent this.

It is also important for you to guard against unauthorized access to your personal information by maintaining strong passwords and protecting against the unauthorized use of your computer or device.

Your California Privacy Rights and California Notice at Collection

This notice to California applicants is provided under the California Consumer Privacy Act (“CCPA”). It supplements and forms a part of Ancestry’s Recruitment Privacy Statement, explains your privacy rights if you are a California resident, and provides certain disclosures required under CCPA.

CCPA refers to “personal information”, which means information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular applicant. “Personal information” excludes de-identified or aggregated applicant or employee information, which Ancestry commits to use in a de-identified form and not attempt to re-identify. It also excludes other information excluded from CCPA’s scope such as health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Fair Credit Reporting Act (FCRA), which governs background checks.

Categories of Personal Information

If you applied for a role with Ancestry within the 12 months prior to the effective date of this notice, Ancestry has collected and collects as personal information, the following categories of personal information in connection with your application for employment:

- Identifiers such as a full name, alias, mailing and/or postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, (and, for successful candidates, social security number, driver’s license number, passport number, visa information) or other similar identifiers, which may be required for employment purposes.
- Sensitive personal information and protected classification characteristics under California or federal law that you voluntarily provide to us including age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, and veteran or military status.
- Professional or employment-related information such as:
    - Personal details and contact information

- Right to work and immigration information
- Talent, recruitment and application details, education, and training details o Work and work history
- Work schedule information
- Requests for accommodation
- Compensation information (if you provided it)
- Benefits elections
- Beneficiary information

We retain this data for as long as necessary to provide services related to your application for employment and related business interests and to comply with legal obligations.

Business Purposes for Collecting Information

We collect this information to perform our obligations related to your application for employment, to comply with legal obligations, and in pursuit of our legitimate business interests in providing services related to your application for employment, including helping to ensure that Ancestry maintains a diverse and inclusive environment for its applicants.

Ancestry does not, and in the 12 months prior to the effective date of this privacy statement has not, sold or shared your personal data, as the terms “sell” and “share” are defined in the CCPA.

Ancestry does not, and in the 12 months prior to the effective date of this privacy statement did not, process personal information, including sensitive personal information, other than to perform its obligations related to your application for employment, to comply with legal obligations and otherwise in pursuit of its related, legitimate business interests.

Categories of Sources of Personal Information

Ancestry collects, and has collected in the 12 months prior to the effective date of this privacy statement, categories of personal information from the following categories of sources:

- Directly from you when you complete Ancestry forms or interact with Ancestry
- Information provided by third parties including from:
  - Ancestry personnel who have referred you for a job
  - Background-checking agencies
  - References that you provide to us
  - Publicly available sources, including any business social media platforms you use or other information publicly available online

Disclosure of Personal Information for Business Purposes

In the 12 months prior to the effective date of this privacy statement, Ancestry has disclosed identifiers, employment-related information, including sensitive personal information, with service providers and contractors acting on our behalf to carry out our legitimate business purposes as described above. For example, we may share your personal information with a recruiting firm to further your candidacy.

Exercising Your Privacy Rights

California residents may exercise the privacy rights described below, subject to limitations in the CCPA.

Right to Know and Access	California residents may request access to categories and specific pieces of personal information that we collect, use, and disclose. Specifically, California residents may request to know and access: The categories of personal information Ancestry has collected about you; The business or commercial purpose for collecting and processing personal information; The categories of sources from which the personal information is collected; The categories of third parties to whom the business discloses personal information; and The specific pieces of personal information it has collected about that consumer.
Right to Delete	California residents may request deletion of personal information that we have collected about them.
Rigth to Correct	California residents may request correction of inaccurate personal information that we have about them.

Ancestry is prohibited from and will not discriminate against you for exercising these California privacy rights.

The most efficient way to access, delete, and correct much of your personal information is to contact peopleops@ancestry.com.