Ancestry Recruitment Privacy Statement

This Recruitment Privacy Statement describes our practices for collecting, storing, and processing of your Personal Information as part of the recruitment process.

What Personal Information Does Ancestry Collect About You?
We will collect Personal Information about you in relation to your job application. 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 may include the following:

Contact Information	Name, email address, physical address, telephone number
Background Information	Resume/CV Employment History Background check details including Criminal History Public records
Demographic Information	Racial or ethnic origin for government reported statistics

How does Ancestry Use and Retain Your Personal Information?
We process your Personal Information for the following purposes:

- to communicate with you about your job application and potential future job opportunities;
- to support and manage the job application process;
- where necessary to comply with applicable legal or regulatory requirements;
- to evaluate and report the demographic makeup of our company where allowed by law; and
- for other purposes as described to you at the time we collect your Personal Information.

Your Personal Information will be retained until the end of the employment application process plus a period of two (2) years. If your job application is successful, the Personal Information collected during the recruitment process will be added to your human resources file and retained for the duration of your employment.

When Does Ancestry Share 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 to provide certain services, such as background checks and relocation vendors;
- To third parties with whom you instruct Ancestry to share your Personal Information;
- We may share your Personal Information if we believe it is reasonably necessary to comply with valid legal process (e.g., subpoenas, warrants) or protect the rights, property, or safety, of Ancestry, our employees or users;
- If Ancestry is acquired or transferred (including in connection with bankruptcy or similar proceedings), 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.

Cookies and Similar Tracking Technologies
Cookies and similar technologies as described in our Cookie Policy. Please refer to our cookie policy to learn about our practices and the controls we provide you.

Access, Correction and Deletion
You may access, correct or delete your Personal Information at any time. To do so, please contact us by using the email address provided below.

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 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 own computer or device.

Data Transfer
Any transfer of your Personal Information between Ancestry's Ireland-based company and Ancestry's U.S.-based company for processing in the United States is conducted pursuant to established transfer mechanisms such as Standard Contractual Clauses or Privacy Shield.

You can request a copy of any standard contractual clauses relating to your Personal Information that we may have executed by contacting us using the details below.

Ancestry and its subsidiaries listed in its certification on the Privacy Shield website comply with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, or Switzerland to the United States. Ancestry has certified to the Department of Commerce that it adheres to the Privacy Shield Principles and that it complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. To learn more about the Privacy Shield program and to view our certification, please visit: https://www.privacyshield.gov/. If there is any conflict between the terms in this Privacy Statement and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

Ancestry's participation in the Privacy Shield applies to all personal data that is subject to the Ancestry Recruitment Privacy Statement and is received from the European Union, European Economic Area, or Switzerland. Ancestry will comply with the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability in respect of such personal data. Ancestry's accountability for personal data that it receives under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, Ancestry remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf (1) do so in a manner inconsistent with the Principles and (2) Ancestry is responsible for the event giving rise to the damage.

We encourage you to contact us as detailed below should you have a Privacy Shield-related (or general privacy-related) complaint. If you are a resident of the European Union, or Switzerland and are dissatisfied with the manner in which we have addressed your concerns about our privacy practices, you may seek further assistance, at no cost to you, from JAMS, our designated Privacy Shield alternative dispute resolution provider based in the United States through the JAMS website at: https://www.jamsadr.com/eu-us-privacy-shield. As further explained in the Privacy Shield Principles, a binding arbitration option will also be made available to you in order to address residual complaints not resolved by any other means. You can learn more about this option through the Privacy Shield website at: https://www.privacyshield.gov/article?id=ANNEX-I-introduction
Ancestry is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Legal basis under EU General Data Protection Regulation for processing personal information of EU residents.
Where you have consented to data processing, your consent provides the legal basis to process your Personal Information. We rely on your explicit consent to process your Personal Information. You have the right to withdraw consent at any time. Please note that your withdrawal of consent to collect and process your Personal Information will not affect the lawfulness of processing your Personal Information based on your consent before you withdrew your consent.

We may also process your Personal Information on the basis of our legitimate interests. Where we rely on legitimate interests to process your Personal Information, you have the right to object to such processing (meaning that you can ask us to stop).

Identity and Contact Details of the Data Controller

If you are applying for a position in the United States, Ancestry.com Operations Inc. and Ancestry.com DNA, LLC are responsible for the use of your Personal Information and for responding to any requests related to your Personal Information.

If you are applying for a position in the European Union, Switzerland or the United Kingdom, Ancestry Ireland Unlimited Company is your data controller. You may also contact the Irish Data Protection Commission, or your local Data Protection Authority with questions.

Please note that if you live outside the United States and are not happy with the way that we have handled your access request, you have a right to complain directly to the Irish Data Protection Commission (for further information see: www.dataprotection.ie) or your local data protection authority. This is in addition to your right to bring a claim before the courts. However, we would welcome the opportunity to try to first resolve any complaint you have in relation to the way we have handled your access request so please let us know if you are not happy with this response.

Contact Information

If you have any questions about this Statement, or the Personal Information we process about you, please contact: dpo@ancestry.com