Candidate Privacy Policy

Last update: November 12, 2021

This Candidate Privacy Policy (the "Policy") details the personal data that Agilent Technologies, Inc. or one of its subsidiaries (collectively, “Agilent Group”, “Company”, “Agilent”, “we”, “us” or “our”) receives about you, how we process it, and your rights and obligations in relation to your personal data. The Agilent entity that is your proposed employer is the data controller for the purposes of applicable law, including but not limited to the General Data Protection Regulation (“GDPR”), the UK General Data Protection Regulation, as supplemented by the UK Data Protection Act 2018 (collectively, "UK Privacy Laws"), the Brazilian General Data Protection Law (the “LGPD”), China’s Personal Information Protection Law, and any other relevant local legislation (“Data Protection Laws”). We are committed to protecting and respecting your privacy.

This policy sets out the basis on which we process any personal data that you provide to us through the Agilent External Careers Site (the “Agilent External Careers Site”) and other data we receive from you or third parties (such as referees) in connection with your job application. Please read the following policy carefully to understand our practices regarding your data and how we will treat it. By using the Agilent External Careers Site you acknowledge the practices described in this policy.

If you have any questions or concerns about this Policy, please contact the Data Protection Officer at:

E-mail: data-protection.officer@agilent.com
Phone: +1 (408) 553 -4417
Post: 5301 Stevens Creek Blvd. Santa Clara, CA 95051

The types of data we receive and use

We will receive and use the following information about you:

- **Information you provide as part of your application.** You will provide us information about you by using our Agilent External Careers Site to apply for a role or by corresponding with us by phone, e-mail, or otherwise. This includes information you provide when you register for and use the Agilent External Careers Site, such as your name, contact information (such as home or work address), date of birth, work experience, educational qualifications, compensation, social security number, and ability to work in the country for which you are applying for employment and any information you choose to submit on or upload to the Agilent External Careers Site (such as information from a CV).

- **Sensitive information you can provide:** Where permitted by local law, you have the option of providing certain sensitive personal data with your consent, such as race or ethnic origin, or whether you have a disability, for the purposes of equal opportunities monitoring. If you decide not to provide this data, your application will not be prejudiced.

- **Information we collect about your usage of the portal.** We automatically collect certain data from you when you use the Agilent External Careers Site, including IP address or other unique device identifiers, information collected by cookies on your usage of the Agilent External Careers Site, mobile carrier (if applicable), time zone setting, operating system and platform, and information regarding your use of the Agilent External Careers Site (“Usage Information”).

- **Information from third parties.** We receive information from third parties in connection with your application, such as referees, recruiters, and organizations that provide background checks (which may include right to work, motor vehicle records and other background checks...
to the extent permitted by applicable law).

**How we use your Information**

The table in Appendix 1 sets out the categories of information we collect, how we use your information, and where applicable, the legal basis for processing relied upon by us under applicable Data Protection Laws to process your personal data.

**How we share your information**

We share your information within the Agilent Group for the purposes set out in Appendix 1. We also share your information with selected recipients for the purposes set out in Appendix 1. These categories of recipients include:

- recruitment portal providers, including ADP;
- IT services providers;
- background check providers;
- travel providers to facilitate interview travel;
- referees;
- administrative services providers including Global Administrative Services Center ("GASC") located in Malaysia; and
- recruitment agencies, including agencies outside of the country and region you reside in.

Where Agilent is under an obligation to do so by law, it will disclose your personal data to regulators, courts, the police or tax/government authorities, or in the course of litigation, in response to an emergency which threatens persons or property, when necessary to protect the legal interests of Agilent, and when required for reasons of national security/prevention or detection of crime. In some cases, in accordance with applicable law, it may not be possible to notify you in advance about the details of such disclosures. Agilent will use all reasonable efforts to disclose the minimum personal data necessary in such cases. All such requests shall be referred to HR and/or Legal Compliance Counsel who may, at their sole discretion, request proof of entitlement and/or exemption under the Data Protection Laws and proof of identity, before releasing any information.

**Where we store your information**

The personal data that we collect from you will be transferred to and stored at/processed in the United States with Agilent Technologies, Inc., and where applicable under the European Commission’s Standard Contractual Clauses for the transfer of personal data to third countries, pursuant to Decisions 2004/915/EC and 2010/87/EU. Please contact the Data Protection Officer should you wish to examine the intra-group Standard Contractual Clauses entered into by Agilent. Agilent uses a number of third-party suppliers (as noted above) to provide services to Agilent. All suppliers that process personal data outside of the EEA or the UK and that are otherwise not located in jurisdictions considered “adequate” by the European Commission shall either (i) have Binding Corporate Rules approved by the relevant supervisory authority; or (ii) are required to execute the Standard Contractual Clauses for the transfer of personal data (pursuant to Decision 2010/87/EU) or otherwise provide evidence of an alternative lawful basis for the transfer of personal data outside of the EEA.

Where the LGPD applies, Agilent will rely on the lawful basis of preliminary procedures related to a contract to transfer personal data to the United States, as well as implement further mechanisms for the safety of these international transfers, as required by the Brazilian Data Protection Authority.
The security of your personal data

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your information transmitted through the Agilent External Careers Site. Once we have received your information, we will take appropriate technical and organizational measures to safeguard your personal data against loss, theft, and unauthorized use, access or modification.

Data retention

If there has been no activity on your candidate profile and information for six months, with the exception of Brazil, Canada, Mexico, Puerto Rico and the US, where your data is stored for four years plus the current year, it will be removed from our database.

Your information will be retained for longer if required by law or a court order and/or as needed to defend or pursue legal claims.

If you are a successful job candidate, your personal data will be retained pursuant to Agilent’s Employee Privacy Notice, which will be provided during your onboarding to Agilent.

Deleting your information

When you deactivate your account, we will still store your data on the Agilent External Careers Site in accordance with the data retention periods stated above. To request deletion of your data, please submit your request to Agilent’s Data Subject Rights Portal [here](#). We reserve the right to retain your data in accordance with the retention period set out above.

Your rights

You have certain rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances and jurisdictions as set out in more detail below. Below, we also set out how to exercise those rights. Please note that we will require you to verify your identity before responding to any requests to exercise your rights. We must respond to a request by you to exercise those rights without undue delay and at least within one month (although this may be extended by a further two months in certain circumstances). Under the LGPD, we will respond to an access and confirmation of processing right within 15 days. To exercise any of your rights, please fill out the following form and submit it [here](#).

Your rights under GDPR and UK Privacy Laws (applicable to candidates in the European Economic Area and the UK)

- **Access.** You have the right to know whether we process personal data about you, and if we do, to access data we hold about you and certain information about how we use it and who we share it with.
- **Portability.** You have the right to receive a subset of the personal data we collect from you in a structured, commonly used and machine-readable format and a right to request that we transfer such personal data to another party. If you wish for us to transfer the personal data to another party, please ensure you detail that party and note that we can only do so where it is technically feasible. We are not responsible for the security of the personal data or its processing once received by the third party. Note: We may not be able to provide you with certain personal data following an access or portability request if providing it would interfere with another individual’s rights (e.g., where providing the personal data we hold about you would reveal information about another person) or where another exemption applies.
- **Correction.** You have the right to require us to correct any personal data held about you that is inaccurate and have incomplete data completed (including by the provision of a
supplementary statement). Where you request correction, please explain in detail why you believe the personal data we hold about you to be inaccurate or incomplete so that we can assess whether a correction is required. Please note that while we assess whether the personal data we hold about you is inaccurate or incomplete, you may exercise your right to restrict our processing of the applicable data as described above. Where we agree that the personal data is inaccurate or incomplete, we will try to tell any third party to whom we have disclosed the relevant data so that they can rectify the data too.

- **Erasure.** You may request that we erase the personal data we hold about you in the following circumstances:
  
  o you believe that it is no longer necessary for us to hold the personal data we hold about you, for instance if you decide that you no longer wish to apply through the Agilent External Careers Site;
  
  o we are processing the personal data we hold about you on the basis of our legitimate interest and you object to such processing. Please provide us with detail as to your reasoning so that we can assess whether there is an overriding interest for us to retain such personal data;
  
  o you no longer wish us to use the personal data we hold about you in order to send you notifications about new positions that match your profile; or
  
  o you believe the personal data we hold about you is being unlawfully processed by us.

Also note that you may exercise your right to restrict our processing of your personal data whilst we consider your request as described below. Please provide as much detail as possible on your reasons for the request to assist us in determining whether you have a valid basis for erasure. We will retain the personal data if there are valid grounds under law for us to do so (e.g., for the defense of legal claims or freedom of expression) but we will let you know if that is the case.

- **Restriction of Processing to Storage Only.** You have a right to require us to stop processing the personal data we hold about you other than for storage purposes in certain circumstances. Please note, however, that if we stop processing the personal data, we may use it again if there are valid grounds under Data Protection Laws for us to do so (e.g. for the defense of legal claims or for another’s protection). Where we agree to stop processing the personal data, we will try to tell any third party to whom we have disclosed the relevant personal data so that they can stop processing the data too. You may request that we stop processing and just store the personal data we hold about you where:
  
  o you believe the personal data is not accurate for the period it takes for us to verify whether the data is accurate;
  
  o we wish to erase the personal data as the processing we are doing is unlawful but you want us to simply restrict the use of that data;
  
  o we no longer need the personal data for the purposes of the processing but you require us to retain the data for the establishment, exercise or defense of legal claims; or
  
  o you have objected to us processing personal data we hold about you on the basis of our legitimate interest and you wish us to stop processing the personal data whilst we determine whether there is an overriding interest in us retaining such personal data.

- **Objection.** You have a right to object to our processing of data about you and we will consider your request. Please provide us with detail as to your reasoning so that we can assess whether there is a compelling overriding interest in us continuing to process such data or we need to process it in relation to legal claims. Also you may request that we restrict processing to storage only whilst we consider your objection.
Your rights under LGPD (applicable to candidates in Brazil)

- **Confirmation, Access and Portability.** You have the right to ask us to access the personal data we hold about you and be provided with certain information about how we use your personal data and who we share it with.

- **Refusal or withdrawal of consent.** You have the right to refuse or to withdraw your consent, however, such fact will not affect the legality of any processing previously carried out. If you refuse or revoke your consent, Agilent may not be able to provide certain services to you. When this is the case, Agilent will let you know.

- **Correction.** You also have the right to ask us to correct your personal data where it is inaccurate or incomplete.

- **Right to deletion, blockage or anonymization.** In certain circumstances, you have the right to ask us to delete, block or anonymize the personal data we hold about you, provided that we do not otherwise have an overriding legitimate basis for processing and/or retaining your personal data.

- **Restriction and Objection.** Where LGPD applies, you are entitled to restrict or to object for specific processing purposes. In some cases, Agilent may demonstrate it has legitimate reasons to process your personal data, which may override your rights, if, for instance, they are strictly essential for the functionality of the services relevant to your relationship with Agilent.

In the event that you wish to make a complaint about how we process your personal data, please contact us in the first instance at data-protection.officer@agilent.com and we will endeavor to deal with your request. This is without prejudice to your right to raise a complaint with a relevant data protection supervisory authority.

**Changes**

We will post any future changes to this policy on this page. Please check back frequently to see any updates or changes to this policy.

**Contact**

Questions, comments and requests regarding this policy are welcomed and should be addressed to the Data Protection Officer at data-protection.officer@agilent.com.
### Purposes for Processing Candidate Data

<table>
<thead>
<tr>
<th>Purpose of Use</th>
<th>Categories of Personal Data Processed for Each Purpose</th>
<th>Legal Basis for Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration of recruitment</td>
<td>Contact details (such as home and work address, phone numbers, email addresses), and curriculum vitae information. Personal information including name, phone number, email address, passport number, seat and meal preference in order to book your travel should you proceed to the interview stage. This includes Categories A, B, C, I and J as enumerated in the definition of “Personal Information” under the California Consumer Privacy Act (“CCPA”).</td>
<td>Necessary for Agilent’s legal obligations (where applicable). Necessary for Agilent’s legitimate interests to assess candidates for employment positions. Necessary for Agilent’s legitimate interests to interview candidates for employment positions.</td>
</tr>
<tr>
<td>To identify and evaluate candidates for employment positions.</td>
<td>Identity information such as title, full name, citizenship, date of birth and proof of eligibility to work (where applicable). Contact details such as home and work address, phone numbers, email addresses, emergency contacts and next of kin information. This includes Categories A, B and C as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to assess candidates for employment positions.</td>
</tr>
<tr>
<td>To determine and validate your qualifications for employment.</td>
<td>Data with respect to education, professional training, and previous career performance including qualifications, certifications, references or curriculum vitae information. This includes Categories A, B, C, I and J as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to assess candidates for employment positions.</td>
</tr>
</tbody>
</table>

---

For California residents, a full list of the types of information that fall within the definition of “personal information” under the CCPA is provided at the end of this Appendix.
<table>
<thead>
<tr>
<th>Purpose of Use</th>
<th>Categories of Personal Data Processed for Each Purpose¹</th>
<th>Legal Basis for Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>To conduct background checks including, to the extent permitted under applicable law (including checking references, qualifications).</td>
<td>Identity and contact information and references from previous employers or professional contacts. Data with respect to educational background and employment history. This includes Categories A, B, C and I as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to assess candidates for employment positions.</td>
</tr>
<tr>
<td>If you are a successful candidate, to create an employment record.</td>
<td>Identity information such as name, gender and date of birth. Contact details such as home and work addresses, phone numbers and email addresses. Personal and family details (such as contact details of spouse/partner and/or children). Data with respect to career commencement and development including date of hire, employee category, and full time or part-time status. Education details, employment details, gender, compensation, bank account details, employee ID, social security number, tax unique identifiers, photo, passport, national ID, religious and political beliefs, trade union membership, health data and criminal conviction data (to the extent permitted by applicable law). This includes Categories A, B, C, I and J as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to onboard successful candidates for employment positions. Necessary for Agilent’s legal obligations (where applicable). Under the LGPD, this is necessary for preliminary procedures related to employment contract.</td>
</tr>
<tr>
<td>To the extent permitted or required by applicable law, to conduct employment and diversity monitoring.</td>
<td>Data relating to race, ethnic origin, nationality or sexual orientation (U.S only not EEA countries or Brazil) This includes Categories A, B and C as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legal obligations (where applicable). Consent (U.S only)</td>
</tr>
<tr>
<td>To provide you with user support of the portal.</td>
<td>Login details such as username and password. This includes Categories A and B as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to assess candidates for employment positions.</td>
</tr>
<tr>
<td>Purpose of Use</td>
<td>Categories of Personal Data Processed for Each Purpose¹</td>
<td>Legal Basis for Processing</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>To communicate with you.</td>
<td>Identity information such as name. Contact details such as home and work addresses, phone numbers and email addresses. This includes Categories A and B as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to assess candidates for employment positions.</td>
</tr>
<tr>
<td>Send you notifications about new positions that match your profile.</td>
<td>Email address.</td>
<td>Necessary for Agilent’s legitimate interests to assess candidates for employment positions.</td>
</tr>
<tr>
<td>To improve the Agilent External Careers Site and to ensure content from the Agilent External Careers Site is presented in the most effective manner for you and your device.</td>
<td>Usage Information, including IP address or other unique device identifiers, information collected by cookies on your usage of the Agilent External Careers Site, mobile carrier (if applicable), time zone setting, operating system and platform, and information regarding your use of the Agilent External Careers Site. This includes Categories A and F as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to offer an effective online platform for recruiting new candidates for employment positions.</td>
</tr>
<tr>
<td>To administer the Agilent External Careers Site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes.</td>
<td>Usage Information, including IP address or other unique device identifiers, information collected by cookies on your usage of the Agilent External Careers Site, mobile carrier (if applicable), time zone setting, operating system and platform, and information regarding your use of the Agilent External Careers Site. This includes Categories A and F as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to offer an effective and secure online platform for recruiting new candidates for employment positions.</td>
</tr>
<tr>
<td>Purpose of Use</td>
<td>Categories of Personal Data Processed for Each Purpose</td>
<td>Legal Basis for Processing</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>To keep the Agilent External Careers Site safe and secure.</td>
<td>Usage Information, including IP address or other unique device identifiers, information collected by cookies on your usage of the Agilent External Careers Site, mobile carrier (if applicable), time zone setting, operating system and platform, and information regarding your use of the Agilent External Careers Site. This includes Categories A and F as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to offer an effective and secure online platform for recruiting new candidates for employment positions.</td>
</tr>
<tr>
<td>To develop the Agilent External Careers Site and improve our recruitment processes.</td>
<td>All data collected from the data subject i.e. identity information, contact details and data with respect to career advancement. This includes Categories A, B, C, F, H, I and J as enumerated in the definition of “Personal Information” under the CCPA.</td>
<td>Necessary for Agilent’s legitimate interests to offer an effective and secure online platform for recruiting new candidates for employment positions.</td>
</tr>
</tbody>
</table>

Under the CCPA, “Personal Information” is information that identifies, relates to, or could reasonably be linked with a particular California resident or household, and includes the following categories of information:

A. Identifiers, such as name, contact information, online identifiers, IP address, Social Security numbers, and other government-issued ID numbers;
B. Personal information, as defined in the California customer records law, such as name, contact information, education information, employment history, financial information, and medical and medical insurance information;
C. Characteristics of protected classifications under California or federal law, such as sex, age, race, religion, national origin, disability, medical conditions and information, citizenship, immigration status, request for leave, and marital status;
D. Commercial information, such as products or services purchased;
E. Biometric information, such as fingerprints and voiceprints;
F. Internet or network activity information, such as browsing history and interactions with our and other websites and systems;
G. Geolocation data, such as device location and IP location;
H. Audio, electronic, visual, and similar information, such as photographs or audio or video recordings created in connection with our business activities;
I. Professional or employment-related information, such as work history, prior employer, information relating to references, details of qualifications, skills and experience, human resources data, and data necessary for benefits and related administration services;
J. Education information subject to the federal Family Educational Rights and Privacy Act, such as student records; and

K. Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual’s preferences and characteristics.

Appendix 2
Processing COVID-19 Vaccination Information

Agilent is a science-based company and believes in the benefits behind COVID-19 vaccinations. To the extent legally permissible, Agilent may ask you about your COVID-19 vaccination status at the time of onboarding and request that you provide proof of full COVID-19 vaccination or documentation of a medical or religious exemption from vaccination (per applicable law). Additionally, in order to be permitted to enter our locations for on-site interviews, we may ask you to show proof of vaccination status. This Appendix 2 is designed to make you aware of our privacy practices with respect to your COVID-19 vaccination information.

I understand that, if I work in a jurisdiction where the collection and processing of health data is restricted:

- I am not required to provide my COVID-19 vaccination status or proof of vaccination. If I choose to do so, it is entirely voluntary.
- If I choose not to disclose my vaccination status, there will be no adverse consequences whatsoever.

<p>| Personal Information We Process | To the extent legally permissible, we may process your name, site location, COVID-19 vaccination status, and either (a) proof of full COVID-19 vaccination; or (b) documentation evidencing a medical or religious exemption from vaccination (per applicable law). |
| Purpose for Processing Your Personal Information | Protecting the health and safety of Agilent personnel from COVID-19 by planning for returning to office in light of health and safety considerations. | Complying with applicable law requiring us to ensure that our personnel is fully vaccinated from COVID-19, as well as our regulatory obligations to protect the health and safety of Agilent personnel, as applicable. |
| How and Where Your Personal Information Will Be Stored | Your information will be stored within Workday. Accessibility to Workday information will be limited to Agilent personnel with a need to know your information. |
| Retention Period for Your Personal Information | We will retain your personal information only as long as necessary, not to exceed 12 months after reporting requirements expire, after which we shall delete your personal information. |
| Legal Basis for Processing | Agilent’s legitimate interest in protecting the health and safety of Agilent personnel, contractors, vendors, customers, and other third parties who visit our locations, as permitted under applicable privacy laws. | Compliance with applicable law requiring us to ensure that our employees are fully vaccinated from COVID-19. |</p>
<table>
<thead>
<tr>
<th>Recipients of the Personal Information</th>
<th>Your personal information will be shared within Agilent and with our processing vendors and contractors on a need-to-know basis. Additionally, we may share your information with governmental bodies only if required under applicable law. Please note that we have not “sold” your personal information. For purposes of this Privacy Notice, “sold” or “sale” means the disclosure of personal information for monetary or other valuable consideration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Border Transfers of Personal Information</td>
<td>As Agilent is a global organization, your information may be shared throughout Agilent’s locations. Please note that all information will be shared pursuant to intragroup agreements between the Agilent entities to protect the cross-border transfer of your information, including (where applicable) the EU Standard Contractual Clauses. Additionally, Agilent engages Workday to collect your information. Please note that Agilent has entered into a data processing agreement with Workday to ensure the protection of your transferred personal information.</td>
</tr>
</tbody>
</table>
| Your Data Subject Rights | Please see below for a list of your applicable rights:  
- You have the right to access the personal information we have about you.  
- You have the right to request correction of your personal information.  
- You have the right to request deletion of your personal information.  
- You have the right to object, on legitimate grounds, to the processing of your personal information.  
- You have the right to limit the use and disclosure of your personal information.  
In order to exercise your rights, please complete the form located here. |
| Rights for California Consumers | If you are a California resident, you may request that we:  
1. Disclose to you the following information covering the 12 months preceding your request:  
   - The categories of personal information we collected about you and the categories of sources from which we collected such personal information;  
   - The specific pieces of personal information we collected about you;  
   - The business or commercial purpose for collecting personal information about you; |
The categories of personal information about you that we sold and the categories of third parties to whom we sold such personal information (if applicable); and

The categories of personal information about you that we otherwise shared or disclosed, and the categories of third parties with whom we shared or to whom we disclosed such personal information (if applicable); and

2. Delete personal information we collected from you.

To make a request for the disclosures or deletion described above, please contact us here or at +1-800-227-9770.

As shown in the linked form, we will need your full name, email address, your relationship to us, and details regarding your request for the purpose of verification. Once we receive your request, we will verify your identity pursuant to regulations under the California Consumer Privacy Protection Act (“CCPA”) by matching the identifying information provided by you to the personal information already maintained by us. We may apply a more stringent verification process depending on the type and sensitivity of the personal information we collect and maintain about you. If we cannot verify your identity from the information we maintain, we may ask for additional information from you, which shall only be used for the purpose of verifying your identity. After verifying your identity, we will respond to your request consistent with applicable law.

Your authorized agent may also submit a request for disclosure or deletion via the aforementioned submission methods. Pursuant to CCPA regulations, we will require the authorized agent to provide the agent’s contact information, information verifying the agent’s identity, and a signed letter of authorization from you that provides your agent with the authority to direct the handling of your personal information.