

DIGICERT CANDIDATE PORTAL ~~EU PRIVACY POLICY NOTICE~~ OVERVIEW

This Privacy Summary is intended to help you understand what data we collect, why we collect it and what we do with it when you apply for a job with us. More information is provided in our [Public Privacy Policy Notice](#). We take your privacy very seriously. Please read this document carefully.

~~Please note that this policy, in its entirety, applies only to residents of the EU who supply personal information to DigiCert through DigiCert's candidate portal.~~

If you submit your job application via InApply on the LinkedIn website, LinkedIn's Terms and Conditions and Privacy Policy will also apply. You can read these on the LinkedIn website.

Data Controllers

DigiCert, Inc., registered at 2801 N Thanksgiving Way, Lehi, UT 84043-5296, United States, and its direct and indirect subsidiaries (“**DigiCert Group**”, “**DigiCert**”, “**we**”, “**us**” or “**our**”) are the data controller, ~~as defined under relevant data privacy law, including for the purposes of~~ the General Data Protection Regulation (“**GDPR**”) ~~in the EU and any other~~ relevant local legislation (“**Data Protection Privacy Laws**”). We are committed to protecting and respecting your privacy. This policy sets out the basis on which we will process any personal data that you provide to us through our career portal (the “**DigiCert Portal**”).

The types of data we receive and how we use it

- **Information you provide as part of your application.** This includes information you provide through the DigiCert Portal (~~either or via LinkedIn~~ or by email), such as your name, contact information, work experience, educational qualifications. Where permitted by local law, you have the option of voluntarily providing certain sensitive personal data (such as race, ~~or~~ ethnicity and disability status) with your consent ~~for the purposes of equal opportunities monitoring. Such information is not used by or available to those who evaluate your application, but is used solely for equal opportunities monitoring as required for US government contractors. We mainly use this to evaluate your application and contact you.~~
- **Information we collect about your usage of the portal.** We automatically collect certain data from you when you use our DigiCert Portal, including your IP address or other unique device identifiers which we use to assess usage of our site, and assist us in developing it.
- **Information from third parties.** We receive information from third parties in connection with your application, such as referees and recruiters, which we use to evaluate your application and verify your credentials.

How we share your information

We will share your information with members of the DigiCert Group for the purpose of processing your application and, if you are successful, creating an employment record.

We will also use third parties to assist us in managing the DigiCert Portal, identifying you and evaluating your application. We will therefore share your information with, for example, background check providers and referees from your previous jobs. A full list of the categories of third parties who may have access to your information is provided [here](#).

Where we store your information

~~Unless you are located in the United States, t~~he information that we collect will be transferred to and stored in locations outside of your country and outside of the European Economic Area (“EEA”). We

take appropriate steps to ensure an adequate level of protection for any of your data that is transferred to another country.

Data Retention

We will retain your information while we are processing your job application and, thereafter, in accordance with our [Public Privacy Policy Notice](#). If you are successful in your application, your data will be retained in accordance with policies applicable to our employees.

Your Rights

You have certain rights in relation to the personal data we hold about you. Some will apply only in certain circumstances. Broadly speaking, these rights pertain to a right of access, portability, correction, erasure, restriction of processing, objection and a right to complain to the relevant [regulatory or](#) supervisory authority.

Contact

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. Questions, comments and requests regarding this policy are welcomed and should be addressed to DigiCert's [HR—People Data Protection—Privacy](#) Champion at people@digicert.com. [General questions regarding DigiCert's privacy policies can also be directed to DigiCert's Data Privacy Officer at dpo@digicert.com.](#)

DigiCert Candidate Portal –~~EU Privacy Policy Notice~~

Data Controllers

DigiCert Parent, Inc., registered at 2801 N Thanksgiving Way, Lehi, UT 84043-5296, United States, and its direct and indirect subsidiaries (including the subsidiaries noted below) (“**DigiCert Group**”, “**DigiCert**”, “**we**”, “**us**” or “**our**”) are the data controller ~~, as defined under relevant data privacy law, including the General Data Protection Regulation (“GDPR”) in the EU and other relevant local legislation (“Data Privacy Laws”).for the purposes of the General Data Protection Regulation (“GDPR”).~~ 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 our careers portal (the “**DigiCert Portal**”) and other data we receive from you or third parties (such as referees) in connection with your job application. Please read the following carefully to understand our views and practices regarding your data and how we will handle it. By using the DigiCert Portals, you acknowledge and agree to the practices described in this policy.

For all data privacy inquiries and any questions or concerns you have about this policy, please contact our ~~HR People Data Protection Privacy~~ Champion (“**Data Privacy Contact**”) at:

E-mail: people@digicert.com

Phone: (801) 896-7973

Post: DigiCert, Inc. Attention ~~HR People Data Protection Privacy~~ Champion, 2801 N Thanksgiving Way, Lehi, UT 84043-5296, USA.

~~Please note that this policy, in its entirety, applies only to residents of the EU who supply personal information to DigiCert through DigiCert’s candidate portal.~~

The types of data we receive and how we use it

We will receive, collect and use information about you when you use the DigiCert Portal, submit a job application to us and, if you are successful, become one of our employees.

Information we collect about your usage of the portal. We automatically collect certain data from you when you use the DigiCert Portal, including IP address or other unique device identifiers, information collected by **cookies** on your usage of the DigiCert Portal, mobile carrier (if applicable), time zone setting, operating system and platform and information regarding your use of the DigiCert Portal (“**Usage Information**”). As it is in our legitimate interests to be responsive to you and to ensure the proper functioning of our products and organisation, we will use your information to:

- improve the DigiCert Portal and to ensure content from the DigiCert Portal is presented in the most effective manner for you and your device;
- administer the DigiCert Portal, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- keep the DigiCert Portal safe and secure; and
- develop the DigiCert Portal and improve our recruitment processes.

Information you provide, and information we collect from third parties, as part of your job application. You will provide us with information about you when you apply for a job with us via the DigiCert Portal. You may submit this information to us either by email ~~or completing the online form~~ or by applying on LinkedIn. All information you submit on LinkedIn in response to our job application

is provided to us and used by us in accordance with this Privacy ~~Policy~~[Notice](#). Please also refer to LinkedIn's Privacy Policy on their website to learn more about how LinkedIn uses your data.

In order for us to process your job application with a view to entering into an employment contract with you, we will ask you to provide information including:

- [Identity Information](#). We will process your name and contact information (e.g., address, phone number, email) to identify you and to correspond with you regarding the job position.
- [Work Experience/Education](#). We will process information about your work experience, educational qualifications, ability to work in the country for which you are applying for employment, personal reference information and any other information you choose to submit on or upload to the DigiCert Portals (such as information from a [resume](#)/CV) for the purpose of evaluating your suitability for the position applied for.
- [LinkedIn Profile](#). If you submit your application via LinkedIn and you have chosen to share your LinkedIn Profile with job posters, we will process data gathered from your LinkedIn profile, including information about your work experience, education, skills and endorsements, accomplishments and any posts you have made public. We will process this information for the purpose of evaluating your suitability for the position applied for. You can amend your privacy preferences for your LinkedIn profile on the LinkedIn website.
- [Background Screening Information](#). We perform background checks on ~~all of our~~ prospective employees [after they have been provisionally offered a position](#). This will include right to work, criminal reference checks and motor vehicle record background checks to the extent permitted by applicable law. For candidates to jobs located in the [USA/United States](#), this will also include drug screening, criminal and credit checks to the extent permitted by applicable law. ~~During the process of your application~~[If you are provisionally offered a position](#), you will be asked to complete an online form for background screening purposes (“**Screening Form**”). We use a [third party vendor, BluebackHireRight](#), to conduct such background screening checks and will share the following information with them:
 - Identity Information
 - Work Experience
 - Certified True Copies of documents proving your identity, for example, a copy of your passport or an identity card
 - Any other information you submit on the Screening Form

Information you may choose to provide for equal opportunities monitoring. Where permitted by local law, you have the option of providing us with certain sensitive personal data, such as, race or ethnic origin, or whether you have a disability. If you provide us with this data, you consent to us using this data for the purposes of equal opportunities monitoring. You can withdraw your consent at any time by contacting us at people@digicert.com. ~~Such information is not used by or available to those who evaluate your application but is used solely for equal opportunities monitoring.~~ If you decide not to provide this data, your application will not be prejudiced.

Information you provide, and information we collect, to keep you informed. As it is in our legitimate interests to communicate with candidates in relation to employment positions applied for and, where applicable, notify applicants of other positions which we think may be of interest to them, we will process your Identity Information to keep you informed in relation to your application and send you notifications of new positions what we think may interest you.

Cookies

We use cookies to enhance your experience using the DigiCert Portal. ~~Cookies are small files which, when placed on your device, enable us to provide certain features and functionality. The DigiCert Portal will detect and use your IP address or domain name for internal traffic monitoring and capacity purposes or to otherwise administer the DigiCert Portal. No personal data is obtained; rather, the patterns of usage of our various users may be tracked to provide you with improved service and content based on aggregate or statistical reviews of user site traffic patterns.~~

~~We use the following cookies:~~

- ~~• Strictly necessary cookies. These are cookies that are required for the operation of the DigiCert Portal. They include, for example, cookies that enable you to log into secure areas of the DigiCert Portal.~~
- ~~• Analytical/performance cookies. They allow us to record patterns of usage of our various users e.g. recognising and counting the number of visitors and to see how visitors move around the DigiCert Portal when they are using it. This helps us to improve the way the DigiCert Portal works, for example, by ensuring that users are finding what they are looking for easily.~~
- ~~• Functionality cookies. These are used to recognise you when you return to the DigiCert Portal. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region).~~

~~If for any reason you wish to not take advantage of cookies, you can disable cookies by changing the settings on your browser. However, if you do so, this may affect your enjoyment of the DigiCert Portal and we will no longer be able to offer to you personalised content. Unless you opt out of cookies, we will consider you consent to the use of cookies. Please see “Cookie Preferences” on DigiCert’s [Cookie Notice](#) website for more information about our use of cookies and how you can exercise control over our use.~~

How we share your information

We use third parties to help us run the DigiCert Portal and help us manage the job applications we receive. We share your information with selected recipients as necessary for them to provide us with their services. We have contracts in place with these third parties and they cannot do anything with you’re your personal data unless we have instructed them to do so. These categories of recipients include:

- ~~• LinkedIn, located in Sunnyvale, California, USA, which we use to host our job applications, and collect and process your information;~~
- IT Services providers including:
 - Greenhouse, located in San Francisco, California, USA, that provides us with recruitment software, and an applicant tracking system, and to collect and process your information;
- background screening providers, including:
 - BluebackHireRight, located in CupertinoIrvine, California, USA, that conducts our background screening checks to verify the information you provide in your application.

We will carry out reference checks by contacting your referees. We will, for the purpose of obtaining an employment reference and verifying information that you have provided to us in your application, contact your named referee and share your name, the position you have applied for and the Work Information you have provided to us.

We will share your information if we are required to do for legal reasons. We will share your information with law enforcement agencies, public authorities or other organizations if such disclosure is reasonably necessary to:

- comply with a legal obligation, process or request;
- enforce our terms and conditions and other agreements, including investigation of any potential violation thereof;
- detect, prevent or otherwise address security, fraud or technical issues; or
- protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection).

We will share your information with a third party involved in any merger, acquisition or asset sale with DigiCert. In the case of a sale, merger or change of control of DigiCert, or in preparation of any of these events, we will share your information with the relevant third party under appropriate obligations of confidentiality.

Where we store your information

The information that we collect from you ~~will~~may be transferred to, and stored in, locations outside of your country and outside of the European Economic Area (“EEA”) as described below.

Transfers within the DigiCert Group

We (your employer) are part of the DigiCert group of companies with our parent company based in the United States, with hub offices in South Africa, Ireland, Japan, India and Australia. As well as in your home country (or within the EEA, if you work within the EEA), your Personal Data will be accessible from and will be transferred to the United States, South Africa, Ireland, Japan, India and Australia, where the DigiCert Group centralizes its data processing and human resources administration.

The DigiCert Group takes all necessary security and legal precautions to ensure the safety and integrity of Personal Data that is transferred within the DigiCert Group. With respect to EU data protection law, DigiCert has executed intra-group agreements between DigiCert entities embodying and incorporating the Standard Contractual Clauses adopted pursuant to European Commission Decisions 2004/915/EC and 2010/87/EU for the lawful transfer of Personal Data under GDPR. Where you have a dispute or complaint regarding DigiCert’s collection, storage, or use of your personal information, you may make a complaint to DigiCert by sending it to people@digicert.com or dpo@digicert.com. Where the dispute or complaint is not satisfactorily resolved or you don’t receive a timely response, if you are an EU resident or where provided by privacy law in your jurisdiction, you may escalate the matter to your European data protection authority or other applicable regulatory authority free of charge, and DigiCert commits to cooperate with the relevant European data protection authority or other applicable regulatory authority and will comply with the advice given by this authority with regard to your information which was transferred from the European Union or your home country in the context of our employment relationship.

~~We are part of the DigiCert Group of companies with our parent company based in the United States. All your personal data will be accessible from and will be transferred to the United States, where the DigiCert Group centralizes its data processing and human resources administration.~~

~~The DigiCert Group takes all necessary security and legal precautions to ensure the safety and integrity of personal data that is transferred within the DigiCert Group. DigiCert has executed intra-group agreements between DigiCert entities embodying and incorporating the Standard Contractual Clauses adopted pursuant to European Commission Decisions 2004/915/EC and 2010/87/EU for the transfer of personal data. Where you have a dispute or complaint regarding DigiCert’s collection, storage, or use~~

~~of your personal information, you may make a complaint to DigiCert by sending it to DigiCert's HR People Data Protection Privacy Champion at people@digicert.com, or DigiCert's Data Privacy Officer at dpo@digicert.com. Where the dispute or complaint is not satisfactorily resolved or you don't receive a timely response, if you are located in the EEA you may escalate the matter to your European data protection authority free of charge, and DigiCert commits to cooperate with the relevant European data protection authority and will comply with the advice given by this authority with regard to your information which was transferred from the European Union in the context of our employment relationship.~~

Transfers to third service providers

Your personal data is also processed by third service providers operating outside the EEA in the United States, who work for us or for one of our suppliers. The personal data is transferred to staff in this country in compliance with the ~~EU-U.S.-E.U.- and Swiss-U.S.~~ Privacy Shield framework, where the third service provider is Privacy Shield certified, or by way of the European Commission's model contracts for the transfer of personal data to third countries (i.e., the standard contractual clauses), pursuant to Decisions 2004/915/EC and 2010/87/EU. Such staff are engaged in, among other things, the processing of your application.

You may request to obtain information about the safeguards that have been put in place by contacting DigiCert's HR Data ~~Protection Privacy~~ Champion by email at people@digicert.com, or ~~DigiCert's Data Privacy Officer at dpo@digicert.com~~. We will take all steps reasonably necessary to ensure that your information is treated securely and in accordance with this policy.

The security of your information

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 DigiCert Portal; any transmission is at your own risk. Once we have received your information, we will take appropriate technical and organisational measures to safeguard your personal data against loss, theft and unauthorised use, access or modification.

How long we store your information

Information we collect about your usage of the portal. ~~We retain this data for 12 months. See the [DigiCert Public Privacy Notice for information about retention of data collected through your use of our website.](#)~~

Information you provide, and information we collect from third parties, as part of your job application. We retain your information for so long as we are evaluating your job application. Thereafter, we retain your information as follows:

- If your job application is successful, we will retain your application information as part of your personnel file. This will be retained in accordance with our Employee ~~Retention Policy Privacy~~ [Notice](#) which will be shared with you as part of the onboarding process.
- If your job application is not successful, we will retain your information for twelve (12) months after notifying you that your application has been unsuccessful and requesting permission to retain your information.

Information you may choose to provide for equal opportunities monitoring. We retain this information for so long as we are evaluating your job application. Thereafter, we retain your information in an aggregated and anonymi~~z~~sed format.

Information you provide, and information we collect, to keep you informed. We retain this data for 12 months.

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.

Your rights

You have certain rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances as set out in more detail below [or in certain jurisdictions as required by applicable Data Privacy Laws](#). 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). To exercise any of your rights, please contact DigiCert's [HR-People](#) Data Protection Champion at people@digicert.com.

- **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 whilst 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 below.
- **Erasure**. You may request that we erase the personal data we hold about you in the following circumstances:
 - 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 submit an application through the DigiCert Portal;
 - -we are processing the personal data we hold about you on the basis of your consent, and you wish to withdraw your consent and there is no other ground under which we can process the personal data;
 - 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;
 - 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
 - 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 defence 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 law~~applicable Data Privacy Laws for us to do so (e.g. for the defence of legal claims or for another's protection). You may request that we stop processing and just store the personal data we hold about you where:
 - you believe the personal data is not accurate for the period it takes for us to verify whether the data is accurate;
 - 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;
 - 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 defence of legal claims; or
 - 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 the 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.

You can withdraw your consent at any time by contacting life@digicert.com or the ~~HR-People~~ Data Protection Champion at people@digicert.com.

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 people@digicert.com (or you can contact our ~~Global Data Protection Privacy Officer Coordinator~~ at gdpr@digicert.com~~dpo@digicert.com~~) and we will endeavour to deal with your request as soon as possible. This is without prejudice to your right to launch a claim ~~with the data protection supervisory authority in the EU~~under applicable Data Privacy Laws to the appropriate regulatory authority in the country in which you live or work where you think we have infringed ~~applicable d~~Data protection Privacy Laws.

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 DigiCert's ~~HR-People~~ Data Protection Champion at people@digicert.com.