



Qlik Recruitment Privacy Notice

At Qlik, two of our Core Values are Open & Straightforward and Take Responsibility. These are particularly relevant for our privacy practices and treatment of personal data. We believe in being Open & Straightforward in our privacy notices about how and why we might process any personal data relating to a specific identifiable person (“Personal Data”) and Taking Responsibility to ensure that Personal Data is safe and only used or shared for legitimate purposes compatible with the reasons it was collected.

The data controller is the entity who determines the purposes and means of the processing of your Personal Data. For Candidates, the data controller is the Qlik legal entity in the country of the job you are applying to. You can find the Qlik company list [here](#). If you have any doubts about the identity of your data controller, please contact us through the means provided in section 10 below.

1. Scope of this Notice

This Qlik Recruitment Privacy Notice (“Notice”) provides information to you as a job candidate for a role with Qlik (“Candidate” or “you”) about Personal Data (including any Sensitive Personal Data, if any – see section 5) the Qlik group of companies (“Qlik”, “us” or “we”) may process about you, including through applying for a job on our recruitment/careers websites, why it is collected, with whom it may be shared, how it is protected, your rights relating to your Personal Data and who to contact with any queries. Please read this Notice in full to understand how Qlik may process your Personal Data. We may update this Notice from time to time and encourage you to check this Notice frequently for any updates.

2. Candidate Personal Data processed by Qlik

The types of Personal Data we process about you may include:

- contact information, such as name, email, home address and phone number;
- CV/resume data such as work history, including previous employer, job title, duties/responsibilities, educational history, as well as any other information submitted by you within or in addition to your CV/resume or provided by you during the interview process;
- background check information, where permitted under local law;
- immigration/right-to-work information (e.g., visa, passport, government ID);
- in compliance with local law, details relating to previous or expected salary and other compensation such as bonus or commission;
- reference information (e.g., from current/previous employer);
- information technology use and traffic information from using or interacting with our systems (e.g., email, phone, video conferencing); and
- image data processing, e.g., by CCTV if your interview is in-person at a Qlik office, or remotely via video conferencing.

Candidate Personal Data may be collected either (i) directly from you, for example via our recruitment/careers’ websites or over interview; and/or (ii) from third parties, such as recruitment agencies, staffing providers, background check providers, referral sources and reference providers. We may also contact you using publicly available sources, such as LinkedIn. Where you have provided Personal Data through a third party (e.g., recruitment agency) you should consult their privacy notices regarding their treatment of your Personal Data



that you have provided to them.

We may also process Personal Data about referees whose contact details Candidates have provided to us ("Referee(s)") so that we may obtain from them reference information about the relevant Candidate.

3. Use of Candidate Personal Data

We will process your Personal Data to:

- assess your application and suitability for a role with Qlik;
- communicate with you about your application, inquiries and to schedule interviews;
- verify your information and, where relevant and permitted by applicable local law, conduct background checks;
- administer our IT systems and premises to interact with you (e.g., by email, phone);
- if you are successful (we wish you the best of luck!), use your Personal Data to offer you a role and enter into an agreement with you;
- manage our recruitment program, such as by analyzing your Personal Data and that of others to improve our recruitment efforts;
- comply with legal requirements, such as immigration and restricted/denied party list checks and equal opportunity employment laws, and
- as otherwise required or permitted by law (e.g., in connection with legal claims, to protect the legal rights, safety or security of Qlik or others, or to otherwise process in connection with compliance, regulatory, auditing/reporting and investigative purposes).

4. Lawful bases for processing

Under the laws of certain countries, we must identify the lawful bases under which we process your Personal Data. These are our legitimate interests (e.g., to assess your application and suitability for a Qlik role, to communicate with you and interview you, to verify your information, to administer our IT systems, manage our recruitment program, safeguard Qlik IT systems and premises, manage legal/compliance matters), to comply with our legal obligations (e.g., immigration/right-to-work checks, checks against restricted/denied party lists, support reasonable adjustment requests), to seek to enter into or perform a contract (i.e., make you an offer and use your information to on-board and employ you) or consent (e.g., if we ask you to keep your information on file for future opportunities with Qlik, or if a Referee chooses to provide us with reference information about a Candidate).

5. Sensitive Personal Data

"Sensitive Personal Data" in this Notice is information defined by applicable local law (e.g., EU/UK GDPR) and considered to be particularly sensitive, such as information relating to health or medical conditions, race or ethnicity, political opinions, religion or philosophical beliefs, trade union membership, genetic or biometric data, or someone's sex life or sexual orientation. In certain countries, in compliance with applicable local law, Qlik will only collect Candidate Sensitive Personal Data where it is strictly necessary due to a legal obligation, such as under local tax, social security, employment or other similar rules, or with the Candidate's explicit consent.

Sensitive Personal Data we may collect about you may include:

- Health information (i) relating to a disability to assess and accommodate any work-related adjustments in



the recruitment process or in the role for which you are applying, and (ii) to ensure the health and safety of the workplace – for example, if you attend an in-person interview at our offices, in light of the Covid-19 pandemic, Qlik may process vaccination or similar information (e.g., negative test) to perform activities such as track-and-trace and office cleaning to reduce the spread of Covid-19, pursuant to local laws and practices;

- Race/ethnicity information where permissible under local employment law. Such information may be collected in certain countries due to legal requirements and for Diversity, Equity and Inclusion monitoring purposes but does not influence hiring or employment decisions;
- Passport or other ID information for the purpose of performing checks as required or permitted under local law (right-to-work, background, etc.); and
- Where permitted by applicable law, Qlik may also collect Sensitive Personal Data for purposes to assist with the achievement of our Diversity, Equity and Inclusion goals. Where required under local law, such Sensitive Personal Data will be collected only with the Candidate’s consent and/or may be anonymized and therefore not considered Personal Data.

6. Sharing your Personal Data

Any sharing of Candidate Personal Data will be done to carry out the uses above. As Qlik is a global business, we may sometimes share your Personal Data across different international Qlik affiliates/successors as well as with third party service providers and advisors in order to fulfil these purposes. Qlik may also share Personal Data as required or permitted under relevant law, for example in the event of a health and safety emergency, with government authorities/law enforcement officials if mandated by applicable law or if required for our legitimate interests, in compliance with applicable laws. If a Qlik business is sold or integrated with another business, your details may be disclosed to our advisers and any prospective purchaser's adviser and to the new owners of the business. Any sharing of Personal Data by Qlik internally within the international Qlik group or with third parties (e.g., recruitment applications portals, video conferencing applications) is protected by Qlik by way of our policies and controls, as outlined in section 8 below.

7. Where we may transfer your Personal Data

As a result of the sharing outlined in section 6 above, your Personal Data may be transferred to another country, such as outside the UK/European Economic Area (e.g., for example if you attend a video interview with a hiring manager in a different country), including for example to the USA, which may not be considered by relevant authorities of your country to have an equivalent level of privacy protection. Qlik will put in place appropriate safeguards for such transfers, for example by using the UK/EU standard contractual clauses or the EU-U.S. Data Privacy Framework.

The U.S. operating affiliates of the Qlik group comply with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce (collectively, the “DPF”). These affiliates have certified to the U.S. Department of Commerce that they adhere to the DPF principles (“DPF Principles”) with regard to the processing of Personal Data received in reliance on the relevant DPF from the EU, EEA, Switzerland and the UK. These affiliates commit to treating all Personal Data received under the relevant DPF in a manner compatible with the DPF Principles.

If there is any conflict between the terms in this privacy notice and the DPF Principles, the DPF Principles shall govern. To learn more about the Data Privacy Framework program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>. To view Qlik’s Data Privacy Framework Policy, please visit <https://www.qlik.com/us/legal/legal-policies>.

8. How Qlik protects your Personal Data



Qlik has robust Security and Privacy programs in place to protect Personal Data. These contain layered policies as well as technical, administrative and physical controls to ensure data is secure and treated in accordance with relevant privacy law, and include the following:

- **Collection & Use:** Personal Data collection must be limited to that necessary to perform the purpose for which it is collected and only be used for the reasons compatible with why it was collected.
- **Confidentiality & Access:** access to Personal Data, within Qlik and by third-party service providers or advisors, must be limited on a least-privilege basis to those who require it for their roles and be kept confidential.
- **Data Retention:** all Personal Data is subject to data retention periods to ensure it is stored for no longer than necessary to perform the purpose for which it was collected. Generally, we will retain Candidate Personal Data for two years, however this may vary depending on your country. If you are successful in your application for the role, your Candidate Personal Data will be retained for longer as it will form part of your HR file and be retained for the duration of your employment until it is eventually deleted under our internal data retention controls.

9. Your rights regarding your Personal Data

You may have certain rights relating to your Personal Data, depending on applicable local law. For example, under UK/EU GDPR and similar laws, you may have the right to:

- request access to and/or obtain a copy of your Personal Data;
- request corrections to your Personal Data if it is inaccurate;
- request further information about the processing of your Personal Data by Qlik;
- request deletion of your Personal Data that is no longer necessary to fulfil the purposes for which it was collected, or does not need to be retained by Qlik for other legitimate purposes;
- where we process your Personal Data on the basis of consent, withdraw this consent at any time. If you ask to withdraw your consent to Qlik processing your Personal Data, this will not affect any processing which has already taken place at that time;
- request a restriction or raise an objection to the processing, sharing and/or further use of your Personal Data;
- if applicable, request that your Personal Data be transferred to another company;
- not be subject to a decision based solely on automated processing which produces legal/significant effects ("Automated Decision-Making");
- not be discriminated against for exercising the above rights; and
- lodge a complaint with your relevant data protection/privacy supervisory.

These rights will depend on the privacy/data protection laws applicable to your Personal Data (typically, where you are resident), the type of Personal Data involved, the reason it is processed, as well as any legal exceptions (e.g., it may not be possible to fulfil a request where it would compromise the confidentiality of Personal Data of others, or where we are required to retain your Personal Data in connection with a legal obligation). We will contact you if we need further information, for example to verify your identity to authenticate your request. We do not generally make recruiting decisions based solely on Automated Decision-Making, however, if we choose to rely solely on Automated Decision-Making that could have a legal/significant impact on you, we will apply the appropriate procedures as may be required by local law, such as providing a mechanism for human



(instead of automated) review. Where legally permitted under relevant law you may designate an authorized agent to submit a privacy request on your behalf. In order to verify this agent request, you will generally need to submit a proof/confirmation that you have authorized this agent to act on your behalf in relating to your privacy rights. For more information regarding your privacy rights, we encourage you to visit the website of your local privacy/data protection authority, such as that of [Brazil](#), [California \(USA\)](#), [EU](#), [Singapore](#) and the [UK](#).

10. Who to contact

To exercise your rights set out in section 9, or for questions about how Qlik processes your Personal Data, please contact Qlik's Data Protection Officer/privacy team at privacy@qlik.com or through the alternate contact details in the [Qlik Privacy & Cookie Notice](#). We are committed to working with you to obtain a fair resolution of any concern or complaint about privacy. However, if you believe that we have not been able to respond to your concern or complaint to your satisfaction, you may where entitled under local law contact your relevant data protection/privacy authority, such as those of the EU (contact details [here](#)) or the UK (contact details [here](#)).