

California Employee, Applicant, and Contractor Privacy Policy

Last Updated: September 30, 2026

Qualfon Data Services Group, LLC and its parents, subsidiaries and affiliates (collectively, "Qualfon," "we," "us," "our") work hard to build and maintain a relationship of trust with you. This California Employee, Applicant, and Contractor Privacy Policy ("Employee Privacy Policy") governs our collection, use, and disclosure of your Personal Information (defined below) in connection with the application and recruitment process, as well as during and after employment or retention as a contractor. This Employee Privacy Policy is not a contract of employment and does not create a promise of continued employment or any particular employment practice. This Employee Privacy Policy applies to California residents only.

This Employee Privacy Policy also explains our practices with respect to Personal Information we collect from and about beneficiaries, dependents, and emergency contacts (collectively, "related parties") of current and former employees and contractors.

Some jurisdictions have different or specific legal requirements governing the use of Personal Information including Personal Information of applicants, employees, and related parties. This Employee Privacy Policy supplements, and does not replace, other notices or policies that may apply to particular systems, forms, benefits, monitoring practices, or jurisdictions. We will comply with all applicable laws and regulations, including local data protection laws.

Employee Privacy Policy Changes

This Employee Privacy Policy is subject to change. We encourage you to review this Employee Privacy Policy frequently for any revisions or amendments. Changes to this Employee Privacy Policy will be posted on this Site and will be effective immediately upon posting. You will be deemed to have been made aware of and have accepted the changes by your continued use of our Site or your continued employment relationship with us. If we determine that a change to this Employee Privacy Policy will result in using your Personal Information acquired before the change being used in a materially new way, we will provide you notice before using your Personal Information in the new way.

INFORMATION WE COLLECT

We collect information that personally identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual ("Personal Information"), including:

- *Identifiers* (e.g., name, title, addresses, telephone numbers, social media profiles, personal email addresses, online identifiers, IP address, account name, Social Security number, driver's license number, passport number, date of birth);
- *Personal Information categories listed Cal. Civ. Code § 1798.80(e)* (e.g., name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, education, employment, employment history, national origin, disability, citizenship, immigration status, medical information);
- *Protected classification characteristics under California or federal law* (e.g., age, race, color, ethnicity, 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, veteran or military status, genetic information (including familial genetic information));
- *Commercial information* (e.g., records of personal property, products or services purchased, obtained, or considered, other purchasing or consuming history or tendencies);
- *Biometric information* (e.g., genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, sleep, health, exercise data, drug test data);
- *Internet or other electronic network activity information* (e.g., browsing history, search history, information about interactions with our website, application or advertisements);
- *Geolocation data* (e.g., physical location indicators from mobile, web, and product that are approximate and/or which are not used to locate a particular individual);

- *Audio, electronic, visual, thermal, olfactory, or similar data* (e.g., call recordings, closed-circuit television recordings, video or audio surveillance, information collected during phone screenings and interviews, photograph for identification purposes (your photograph will not be used to create a biometric identifier or biometric template), information collected from our review of your use of (i) Qualfon systems such as email, project management software, and communication platforms, (ii) Qualfon-authorized devices such as computers, tablets, telephones, and (iii) Qualfon-issued equipment and vehicles);
- *Professional/employment-related information* (e.g., employer, job title, work history, details regarding the type of employment sought, desired salary, willingness to relocate, job preferences, and other information related to compensation and benefits, reference information (including information provided by third parties), insurance and other benefits enrollment information, beneficiary and emergency contact information, bank account details and payroll information, drug test history and results, physical or mental health condition or disability status (to determine appropriate workplace accommodations and evaluate fitness for a particular position), marital and dependent status when needed to administer benefits such as health insurance or pension benefits, and other relevant experience including information contained in a resume, CV, cover letter, job application);
- *Education information* (e.g., student records, degrees awarded, transcripts, and other information provided in support of the job application); and
- *Inferences drawn from other Personal Information* (e.g., background check reports and drug test reports);

We also collect certain types of Personal Information which California law treats as sensitive ("Sensitive Personal Information"), such as:

- *Government identifiers* (e.g., social security, driver's license, state identification card, and passport number);
- *Complete account access credentials* (e.g., usernames, account numbers, or card numbers combined with required access/security code or password);
- *Precise geolocation* (e.g., a geographic area used to locate an individual that is equal to or less than the area of a circle with a radius of 1,850 feet);
- *Racial or ethnic origin*;
- *Citizenship or immigration status*;

- *Religious or philosophical belief;*
- *Union membership;*
- *Biometric information used to uniquely identify an individual;*
- *Health information such as diagnosis or disability;*
- *Sex life information or sexual orientation; and*
- *Communications not directed to us such as mail, email, or text message content where we are not the intended recipient.*

HOW WE COLLECT PERSONAL INFORMATION

Voluntary Disclosure From You

In most cases, we will collect the Personal Information that we use directly from you.

Third Parties

In some circumstances third parties may provide your Personal Information to us, such as former employers, medical professionals, and/or insurers, or in connection with a background, employment, or reference check, subject to your consent where required by law.

Qualfon-Authorized Equipment & Systems and Communication Recordings

We and our Service Providers may collect, use, and disclose Personal Information from our review of your use of (i) Qualfon systems such as email, project management software, and communication platforms, (ii) Qualfon-authorized devices such as computers, tablets, telephones, and (iii) Qualfon-issued equipment and vehicles.

We and our Service Providers may record and retain your usage of, and contents within, Qualfon-authorized devices such as computers, tablets, telephones. By using such devices, you consent to our and our Service Providers recording and retention of your usage and the contents within. You understand that you have no expectation of privacy when using Qualfon-authorized devices.

Employee Through Whom a Beneficiary Receives Benefits

If you are not employed by us, but receive benefits through one of our employees, are a dependent of an employee, or serve as an employee or contractor's emergency contact, we may collect Personal Information from the employee or contractor with whom you have a relationship.

HOW WE USE AND DISCLOSE PERSONAL INFORMATION

Generally

We may use your Personal Information for business purposes, such as:

- Verifying your information and carrying out employment, background, and reference checks, subject to your consent where required by applicable law.
- Verifying your eligibility for employment and, if applicable and required, supporting you with obtaining a work permit or visa.
- Keeping records related to our hiring processes, for only as long as appropriate under the circumstances.
- Onboarding you as a new employee or contractor.
- Creating and submitting reports as required by applicable laws or regulations.
- To comply with our legal, regulatory, or other corporate governance requirements.
- Analyzing and improving our application and recruitment process and practices.
- Payroll/payment administration.
- Benefits administration.
- Business management and planning.
- Processing employee work-related claims (for example, insurance claims).
- Accounting and auditing.
- Conducting performance reviews and determining performance requirements.
- Assessing qualifications for a particular job or task.
- Gathering evidence for disciplinary action or termination.

- Complying with applicable laws, regulations, and corporate governance requirements.
- Education, training, and development requirements.
- Complying with health and safety obligations.
- To prevent fraud.
- To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems, working from an unauthorized physical location, and preventing malicious software distribution.
- To ensure physical security of our personnel, offices, stores, and equipment.
- To evaluate or facilitate business transactions such as a merger, acquisition, or asset sale.

We use Sensitive Personal Information in the context of the employer-employee relationship as described above and do not use or disclose it for any purposes beyond those allowed in 11 Cal. Code of Regs. § 7027(m).

Personal Information Disclosures

We may disclose your Personal Information for employment-related purposes to:

- Employees, contractors, or designated agents who require such information to assist us with administering our relationship with you.
- Service providers who require such information to assist us with administering our relationship with you, including service providers who provide services to us or you or on our behalf. Service providers may include, but are not limited to, payroll/payment processors, benefits administration providers, professional employment organizations, background check providers, and data storage or hosting providers. These service providers may be located outside of your home jurisdiction. We do not permit our service providers to use your Personal Information for their own purposes. We only permit them to use your Personal Information for specified purposes in accordance with our instructions.
- Third parties where required by law, to protect our rights and property and the rights of property of any related companies, during emergency situations or where necessary to protect the health or safety of persons, or If a

business transfer or change in ownership occurs and the disclosure is necessary to complete the transaction.

In the past twelve months, we have disclosed the following categories of Personal Information to the following categories of third parties who are not our service providers ("Third Parties"):

- Government officials: Identifiers (name, address, and employee ID)
- Law enforcement and courts: Identifiers (none)
- Parties to litigation: Identifiers (name and employee ID)

Selling And Sharing Personal Information

We do not sell or share Personal Information of any applicants, current or former employees, contractors, beneficiaries, dependents, or emergency contacts, including of persons under 16 years of age, to third parties. We also do not share such information for cross-context behavioral advertising purposes.

Security

We recognize the importance of safeguarding the confidentiality of Personal Information from loss, misuse, or alteration. Accordingly, we employ commercially reasonable administrative, technical, and physical safeguards to protect such Personal Information from unauthorized access, disclosure, and use. Even with these safeguards, no data transmission over the Internet or other network can be guaranteed 100% secure. As a result, while we strive to protect information transmitted on or through our Site or Services, you do so at your own risk.

Employee and Contractor Responsibilities. Employees and contractors must follow Qualfon's information-security, acceptable use, records management, and incident reporting requirements and must not submit confidential employee, client, customer, or Qualfon information to unauthorized applications or artificial intelligence tools.

Data Retention

We keep your Personal Information for as long as needed or permitted considering the purpose(s) for which it was obtained. The criteria used to determine our retention periods include (i) for as long as we have an ongoing relationship with you; (ii) as required by a legal obligation to which we are subject; or (iii) as advisable in light of

our legal position (such as in regard of applicable statutes of limitations, litigation, or regulatory investigations).

If you are offered and accept employment or a contractor relationship with us, the Personal Information we collected during the application and recruitment process will become part of your employment or contractor record, and we may use it in connection with your relationship with us consistent with our policies. If you do not become an employee or contractor, or, once you are no longer an employee or contractor of us, we will retain and destroy your Personal Information in accordance with our document retention policies and applicable laws and regulations.

Updating Your Information

It is important that the Personal Information we hold about you is accurate and current. Please contact us at person.office@qualfon.com if your Personal Information changes during the application process or during your employment.

Additional California Consumer Rights

If you are an applicant, employee, or contractor or a beneficiary, dependent, or emergency contact of such a person residing in California you have additional rights to access and control your Personal Information. Exemptions may apply. Consumer privacy rights include:

Right to Know

You have the right to request twice per 12-month period that we disclose to you certain information about our collection, use, disclosure, and sale of your Personal Information over the past 12 months, including: (i) the categories or, if requested, specific pieces of Personal Information we collected about you; (ii) the categories of sources from which your Personal Information was collected; (iii) the business or commercial purpose(s) for which we collected or sold your Personal Information; and (iv) the categories of Third Parties with whom we sold, shared, or disclosed your Personal Information, including the categories of Personal Information sold, share, or disclosed to each and the purposes for doing so. We are not permitted to provide access to specific pieces of Personal Information that creates a high risk of potential harm from disclosure to an unauthorized person such as financial information, social security numbers, and driver's license numbers. We will not provide specific pieces of Personal Information unless you expressly request them.

Right to Delete

You have the right to request that we delete any Personal Information we have collected about you. Please understand that we are not required to honor a deletion request if a legal exemption applies such as if we need the information to complete a requested or reasonably anticipated transaction, prevent security incidents or fraud, or comply with legal obligations. We will retain a copy of your deletion request for at least two years as required by law.

Right to Correct

You have the right to request that we correct inaccurate Personal Information we maintain about you. After you request to correct inaccurate Personal Information, we will provide instructions for you to provide us with optional documentation to support your request and we will consider it. We may decline to correct your Personal Information if we determine based on the totality of the circumstances that your Personal Information is more likely than not accurate. We may also decline to correct your Personal Information if we determine that your request is fraudulent or abusive. We may decide to delete your allegedly inaccurate personal information instead of correcting it.

If you only wish to update your contact information or other Personal Information rather than disputing its accuracy, please refer to the Updating Your Information section above.

Submitting a Request

You may submit a request through our [consumer privacy choices form](#) by calling us at (888) 380-2190. After you submit your request via the methods described above, we may contact you to obtain additional information necessary to verify your identity. For example, we may require you to verify certain information in our files or submit a signed declaration under penalty of perjury verifying your identity. We will not process your request without verifying your identity, so please respond promptly. If you do not timely respond to our requests for information, we may deny your request.

We will process verified Right to Know, Right to Correct, and Right to Delete requests within 45 days of receipt, subject to any applicable exemptions and extensions permitted by law up to 90 days.

Authorized Agent

If you are an authorized agent submitting a request for another California resident, you must provide a written authorization from the consumer (along with proof of your identity) or a copy of a lawful power of attorney. You may provide this documentation via email at consumerprivacy@qualfon.com after submitting the request. We may contact you or the consumer on whose behalf you claim to act to verify your authorization.

Non-Discrimination

We will not discriminate or retaliate against any person who exercises their privacy rights under applicable law or this Employee Privacy Policy.

Not A Contract Of Employment

This Employee Privacy Policy does not create a contract for employment, compensation, hours of work, or for the provision of benefits. If you are a current employee, you are employed at-will, without any definite term or duration, and your employment with us can be terminated at any time, by either party, for any or no reason.

Contact Us

If you have any questions about privacy requests, please email us at consumerprivacy@qualfon.com or call us at (888) 380-2190.

For general questions regarding our Employee Privacy Policy, please email us at privacy@qualfon.com, call us at (888) 380-2190 or send us a letter to the following address:

Qualfon
Attn: Chief Compliance Officer
13700 Oakland Avenue
Highland Park, MI 48203