Contents

Consumers, Applicants and Contractors Online Privacy Policy ........................................ 3
Worksite Employee Privacy Policy ................................................................. 14
Employee Privacy Policy ........................................................................ 25
Consumers, Applicants and Contractors Online Privacy Policy

CoAdvantage Corporation (the “Company” or “we”) has developed this privacy policy out of respect for the privacy of our customers, visitors to our website, job applicants, and independent contractors. This policy describes the personal information we collect, use, and disclose about individual consumers, applicants, and contractors who visit or interact with this website, visit any of our offices, stores, facilities or locations, purchase or inquire about any of our products or services, contract with us to provide services, apply for a position of employment, or otherwise interact or do business with us.

Whenever you visit our website, we will collect some information from you automatically simply by you visiting and navigating through this site, and some voluntarily when you submit information using a form on the website, enroll in or subscribe to our newsletter or marketing communications, request information, or use any of the other interactive portions of our website. Through this website, we will collect information that can identify you and/or your activity.

Additionally, whenever you communicate, interact or do business with us, whether online or at any of our physical locations or facilities, or whether you are contracted to perform services for us or apply for a position of employment, we will be collecting personal information from you or about you in the course of our interaction or dealings with you.

This policy does not apply to our current and former employees and their family members, dependents, and beneficiaries; if you are a California resident who is a current or former employee of the Company or a family member, dependent, or beneficiary of any of our current or former employees.
**Collection of Personal Information and Sensitive Personal Information**

In the last 12 months, we have collected the following categories of personal information about you based on your specific transactions and interactions with us or our website. For each category of information, the categories of third parties with whom we have disclosed the information in the last 12 months are referenced by a letter that coincides with the letter in the list of categories of service providers and third parties that follows soon after this table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Disclosed in Last 12 Months To</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Identifiers</td>
<td>Name, alias</td>
<td>K</td>
<td>Duration of our relationship with you plus 7 years</td>
</tr>
<tr>
<td>Contact Information</td>
<td>Home, postal or mailing address, email address, home phone number, cell phone number</td>
<td>I, K</td>
<td>Duration of our relationship with you plus 7 years</td>
</tr>
<tr>
<td>Account Information</td>
<td>Username and password for Company accounts and systems, and any required security or access code</td>
<td>Not Disclosed</td>
<td>Duration of relationship with you plus 7 years</td>
</tr>
<tr>
<td>Commercial Transactional Data</td>
<td>Information regarding products or services provided, purchasing history.</td>
<td>A, B, C, E, F, G, H, M</td>
<td>7 years after last service/transaction, unless necessary to maintain for a longer period for product warranty, or OSHA/ FDA or other regulatory compliance</td>
</tr>
<tr>
<td>Internet Network and Computer Activity</td>
<td>Date and time of your visit to this website; webpages visited; links clicked on the website; browser ID; browser type; device ID; form information downloaded; and cookies.</td>
<td>F, H, L</td>
<td>2 years</td>
</tr>
<tr>
<td>Geolocation Data</td>
<td>IP address</td>
<td>L</td>
<td>2 years</td>
</tr>
<tr>
<td>Mobile Device Data</td>
<td>Information collected when you navigate, access or use any of our websites via mobile device.</td>
<td>B, E, F, H</td>
<td>2 years</td>
</tr>
<tr>
<td>Financial / Employment Data</td>
<td>Information collected through including employment history, company name, role, salary, dates of employment.</td>
<td>I, J, K</td>
<td>If hired, this data will be retained for duration of employment plus 7 years; if not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.</td>
</tr>
<tr>
<td>Inferences</td>
<td>Based on analysis of your activity on the website, we may develop inferences regarding your interest in our products/services and potential for purchasing.</td>
<td>B, E, F, H</td>
<td>Duration of our relationship with you plus 4 years</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td>Disclosed in Last 12 Months To</td>
<td>Retention Period</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Online Portal and Mobile App Access and Usage Information</td>
<td>Username and password, account history, usage history and file access logs.</td>
<td>L</td>
<td>Duration of our relationship with you plus 7 years</td>
</tr>
<tr>
<td>Visual, Audio or Video Recordings</td>
<td>Your image when recorded or captured in surveillance camera footage or pictures of you taken on our premises or at our events or that you share with us.</td>
<td>L, I</td>
<td>Surveillance video – 90 days; duration of our relationship with you plus 4 years</td>
</tr>
<tr>
<td>Pre-Hire Information</td>
<td>Information gathered as part of background screening and reference checks, pre-hire drug test results, information recorded in job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you.</td>
<td>I, J, K</td>
<td>If hired, this data will be retained for duration of employment plus 7 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.</td>
</tr>
<tr>
<td>Employment and Education History</td>
<td>Information contained in your resume regarding educational history, information in transcripts or records of degrees, vocational certifications obtained, and information regarding prior job experience, positions held, and when permitted by applicable law your salary history or expectations.</td>
<td>I, J, K</td>
<td>If hired, this data will be retained for duration of employment plus 7 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.</td>
</tr>
<tr>
<td>Professional Related Information</td>
<td>Information contained in tax forms/1099 forms, licensing and certification records, and performance records, and information related to services provided by independent contractors, including in statements of work.</td>
<td>A, I, J, K</td>
<td>Duration of our relationship with you plus 7 years</td>
</tr>
<tr>
<td>Facility &amp; Systems Access Information</td>
<td>Information identifying you, if you accessed our secure company facilities, systems, networks, computers, and equipment, and at what times, using keys, badges, fobs, login credentials, or other security access method.</td>
<td>L</td>
<td>Duration of our relationship with you plus 7 years</td>
</tr>
</tbody>
</table>
Of the categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect from or about consumers, independent contractors, or applicants:

**Sensitive Personal Information Categories**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Identifiers</td>
<td>social security number, driver’s license or state identification card number, passport number</td>
</tr>
<tr>
<td>Account Information</td>
<td>your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account</td>
</tr>
<tr>
<td>Protected Classifications</td>
<td>racial or ethnic origin, religious or philosophical beliefs, union membership, or sexual orientation</td>
</tr>
<tr>
<td>Geolocation Data</td>
<td>IP address and/or GPS location, latitude &amp; longitude</td>
</tr>
</tbody>
</table>

**Personal Information DOES NOT include:**

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer, independent contractor, or applicant, or from widely distributed media.
- Information made available by a person to whom the consumer, independent contractor, or applicant has disclosed the information if the consumer, independent contractor, or applicant has not restricted the information to a specific audience.
- Deidentified or aggregated information.

**We may collect your personal information from the following sources:**

- You the consumer, independent contractor, or job applicant, when you visit the website and voluntarily submit information through forms on the website or social media, when you visit any of our stores or physical locations, when you purchase or inquire about any of our products or services, when you enter into a contract to perform services for us, or when you apply for a position of employment
- Our employees and contractors, when you interact with them
- We utilize cookies to automatically collect information about our website visitors
- Surveillance cameras at our physical locations
- Lead generators and referral sources
- Credit and consumer reporting agencies
- Recruiters
- Social media platforms
- Company systems, networks, software applications, and databases you log into or use
We may disclose your personal information to the following categories of service providers, contractors, or third parties:

A. Financial institutions
B. Lead providers
C. Product manufacturers/administrators
D. [Intentionally Omitted]
E. Promotional or other fulfillment vendors
F. Support vendors for marketing and sales, managing or hosting the website
G. Transaction support vendors (e.g., check guaranty, payment processors)
H. Data analytics vendors
I. Professional employer organizations
J. Consumer reporting agencies or credit reporting agencies
K. Employee tracking and talent management systems
L. Security and risk management vendors
M. Corporate customers

We may collect your personal information for the following business purposes:

1. To fulfill or meet the purpose for which you provided the information.
2. [Intentionally omitted].
3. To process, complete, and maintain records on transactions.
4. [Intentionally omitted].
5. To retain your selection for Email opt in/opt out to ensure customers who opted out are not sent any Email messages.
6. [Intentionally omitted].
7. To schedule, manage and keep track of customer appointments.
8. To complete quotes for services.
9. To maintain records of when customers decline a service or sale.
10. To respond to consumer inquiries, including requests for information, customer support online, phone calls, and in-store inquiries.
11. To provide interest-based and targeted advertising.
12. To improve user experience on our website.
13. To understand the demographics of our website visitors.
14. To detect security incidents.
15. To debug, identify, and repair errors that impair existing intended functionality of our website.
16. To protect against malicious or illegal activity and prosecute those responsible.
17. To verify and respond to consumer requests.
18. To prevent identity theft.
19. JOB APPLICANT PURPOSES:
   a. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to apply for a job with the Company, we will use that Personal Information in connection with your candidacy for employment.
   b. To comply with local, state, and federal law and regulations requiring employers to maintain certain records, as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.
   c. To evaluate your job application and candidacy for employment.
   d. To obtain and verify background check and references.
   e. To communicate with you regarding your candidacy for employment.
   f. To reduce the risk of spreading infectious diseases in or through the workplace.
20. INDEPENDENT CONTRACTOR PURPOSES:
   a. To fulfill or meet the purpose for which you provided the information.
   b. To comply with state and federal law and regulations requiring businesses to maintain certain records (accident or safety records, and tax records/1099 forms).
   c. To engage the services of independent contractors and compensate them for services.
   d. To evaluate, make, and communicate decisions regarding an independent contractor, including decisions to hire and/or terminate.
   e. To grant independent contractors access to secure Company facilities, systems, networks, computers, and equipment, and maintain information on who accessed such facilities, systems, networks, computers, and equipment, and what they did therein or thereon.
   f. To implement, monitor, and manage electronic security measures on independent contractor devices that are used to access Company networks and systems.
   g. To evaluate, assess, and manage the Company’s business relationship with vendors, service providers, and contractors that provide services to the Company.
   h. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
   i. To reduce the risk of spreading infectious diseases in or through the workplace.

We may disclose your personal information for the following business purposes as numbered above:
1, 3, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19(a), 19(b), 19(d), 20(a), 20(e), 20(f), 20(g), 20(h), and 20(i).

We do NOT and will not sell your personal information in exchange for monetary or other valuable consideration. We do not share your personal information for cross-context behavioral advertising.

We do not and will not use or disclose your sensitive personal information for purposes other than the following:

1. To perform the services reasonably expected by an average consumer, applicant or contractor who requests those services.
2. To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
3. To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
4. To ensure the physical safety of natural persons.
5. For short-term, transient use.
6. To perform services on behalf of the Company.
7. To verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company.
8. For purposes that do not involve inferring characteristics about the consumers, contractors, and applicants.
Retention of Personal Information
We will retain each category of personal information in accordance with our established as indicated above. In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statutes of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

Third Party Vendors
We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail services and running special promotions. Such parties only have access to the personal information needed to perform these functions and may not use or store the information for any other purpose. Subscribers or site visitors will never receive unsolicited e-mail messages from vendors working on our behalf.

Business Transfers
In the event we sell or transfer a particular portion of our business assets, information of consumers, contractors and applicants may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, information of consumers, contractors and applicants may be transferred as part of the acquisition.

Compliance with Law and Safety
We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Use of Cookies and Other Tracking Technologies
Cookies are small files that a website may transfer to a user’s computer that reside there for either the duration of the browsing session (session cookies) or on a permanent, until deleted, basis (persistent cookies) that may be used to identify a user, a user’s machine, or a user’s behavior. We make use of cookies under the following circumstances and for the following reasons:

• Provide you with services available through the website and to enable you to use some of its features
• Authenticate users and prevent fraudulent use of user accounts
• Identify if users have accepted the use of cookies on the website
• Compile data about website traffic and how users use the website to offer a better website experience
• Understand and save visitor preferences for future visits, such as remembering your login details or language preference, to provide you with a more personal experience and to avoid you having to re-enter your preferences every time you use the website
• Track your browsing habits to enable us to show advertising which is more likely to be of interest to you, including advertising by third parties on our website

You may delete cookies from your web browser at any time or block cookies on your equipment, but this may affect the functioning of or even block the website. You can prevent saving of cookies (disable and delete them) by changing
your browser settings accordingly at any time. It is possible that some functions will not be available on our website when use of cookies is deactivated. Check the settings of your browser. Below you can find some guidance:

- **Safari**
- **Opera**
- **Internet Explorer**
- **Google Chrome**
- **Mozilla**

**External Links**

Our website contain links to other sites. We are not responsible for the privacy practices or the content of such websites. To help ensure the protection of your privacy, we recommend that you review the Privacy Policy of any site you visit via a link from our website.

**Passwords**

The personal data record created through your registration with our website can only be accessed with the unique password associated with that record. To protect the integrity of the information contained in this record, you should not disclose or otherwise reveal your password to third parties.

**Children Under the Age of 16**

We do not knowingly sell or share the personal information of consumers under 16 years of age.

**How We Protect the Information We Collect**

The protection of the information that we collect about visitors to this website is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We use internal encryption on all data stores that house voluntarily captured data.
- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- We restrict access to private information to those who need such access in the course of their duties for us.

**International Visitors**

We do not target, market to, or offer our products or services to consumers outside of the United States. You agree not to submit your personally identifiable information through the website if you reside outside the United States.
**Rights Under the CCPA and CPRA**

This section of the Privacy Policy applies only to California residents who are natural persons; it does not apply to any entities (whether business, non-profit or governmental). If you are a California resident, you have the following rights:

<table>
<thead>
<tr>
<th>Right to Know</th>
<th>The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected about you going back to January 1, 2022, unless doing so would be impossible or involve disproportionate effort, or unless you request a specific time period, (2) the categories of sources from which the personal information was collected, (3) the business or commercial purpose for collecting, selling, or sharing this information, (4) the categories of third parties with whom we share or have shared your personal information,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to Access</td>
<td>The right to request, up to 2 times in a 12-month period, that we disclose to you, free of charge, the specific pieces of personal information we have collected about you going back to January 1, 2022, unless doing so would be impossible or involve disproportionate effort, or unless you request a specific time period;</td>
</tr>
<tr>
<td>Right to Delete</td>
<td>The right to request, up to 2 times in a 12-month period, that we delete personal information that we collected from you, subject to certain exceptions;</td>
</tr>
<tr>
<td>Right to Correct</td>
<td>The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;</td>
</tr>
<tr>
<td>Right to Designate</td>
<td>The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and</td>
</tr>
<tr>
<td>Right to Not be Discriminated or Retaliated Against</td>
<td>The right to not be discriminated or retaliated against for exercising any of the above rights, including an applicant’s and independent contractor’s right not to be retaliated against for exercising the above rights.</td>
</tr>
</tbody>
</table>

You can submit any of the above types of consumer requests through any of the 2 options below:

- Submit an online request at: [https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03](https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03)
- Call our privacy toll-free line at 800-868-1016

**How We Will Verify That it is Really You Submitting the Request**

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular records in our possession, which depends on the nature of your relationship and interaction with us. For example, we may need you to provide your name, email, phone number, IP address, browser ID, amount of your last purchase with the business, and/or date of your last transaction with the business.
Responding to Your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we believe the request is fraudulent.

If You Have an Authorized Agent

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf, and we will also contact you and ask you for information to verify your own identity directly with us and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Other California Privacy Rights

The California Civil Code permits California Residents with whom we have an established business relationship to request that we provide you with a list of certain categories of personal information that we have disclosed to third parties for their direct marketing purposes during the preceding calendar year. The Company does not disclose any information to third parties for their direct marketing purposes.
Consent to Terms and Conditions
By using this website, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy
As our services evolve and we perceive the need or desirability of using information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check our website frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Privacy Policy, we will post the revised Privacy Policy and the revised effective date on this website. Please check back here periodically or contact us at the address listed at the end of this Privacy Policy.

Consumers With Disabilities
This policy is in a form that is accessible to consumers with disabilities.

Questions About the Policy
This website is owned and operated by CoAdvantage. If you have any questions about this Privacy Policy, please contact us at 800-868-1016 or submit an inquiry to https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03

**This policy was last updated December 31, 2022.**
Worksite Employee Privacy Policy

CoAdvantage Corporation and its affiliated companies (the “Company” or “we”) has developed this Privacy Policy out of respect for the privacy of worksite employees. This Policy describes the personal information we collect, both online and offline, and that we use and disclose about worksite employees. We will collect some information from you for various purposes.
Collection of Personal Information and Sensitive Personal Information

In the last 12 months, we have collected the following categories of personal information from or about worksite employees, including information about worksite employees’ family members, dependents, and beneficiaries. For each category of information, the categories of third parties to whom we have disclosed, sold, or shared the information within the last 12 months are referenced by a letter that coincides with the letter in the list of categories of service providers and third parties that follows soon after this table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Disclosed in Last 12 Months To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Identifiers</td>
<td>Name, alias, social security number, date of birth, driver’s license or state identification card number, passport number, permanent resident alien card number, alien registration receipt, employment authorization document number, school ID, voter’s registration card number, U.S. military card number, draft record, military dependent ID number, native American tribal document number, school record, report card, clinic, doctor or hospital record, daycare or nursery school record, birth certificate, certifications of report of birth document, U.S. citizen ID card number and employee ID number.</td>
<td>A, B, C, D, E, F, I, J</td>
</tr>
<tr>
<td>Contact Information</td>
<td>Home, postal or mailing address, email address, home phone number, cell phone number emergency contact number.</td>
<td>A, B, C, D, E, F, I, J</td>
</tr>
<tr>
<td>Account Information</td>
<td>Username and password for Company accounts and systems, and any required security or access code, password, or credentials allowing access to your Company accounts.</td>
<td>J</td>
</tr>
<tr>
<td>Protected Classifications</td>
<td>Race, ethnicity, national origin, sex, gender, sexual orientation, gender identity, religious or philosophical beliefs, age, physical or mental disability, medical condition, veteran or military status, familial status, language, or union membership.</td>
<td>B, C, D, E, F, I</td>
</tr>
<tr>
<td>Physical Characteristics or Description</td>
<td>Information on your Driver’s License (such as eye color, hair color, height, weight), as well as information collected to the extent relevant for the workplace.</td>
<td>B, C, D, F, I</td>
</tr>
<tr>
<td>Visual Audio, Video Recordings</td>
<td>IP addre Your image when recorded or captured in surveillance camera footage or pictures of you taken on our premises or at your worksite employer’s premises or that you share with us.</td>
<td>B, C, D, F, I</td>
</tr>
<tr>
<td>Financial Information</td>
<td>Bank account number for direct deposit, or other financial account information.</td>
<td>A, B, F</td>
</tr>
<tr>
<td>Pre-Hire Information</td>
<td>Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, job interview notes by persons conducting job interviews for Company’s customer (worksite employer), information contained in candidate evaluation records and assessments, information in work product samples you provided, voluntary disclosures by you, and Wage Opportunity Tax Credit (WOTC) information.</td>
<td>A, B, D, E, F, I, K</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td>Disclosed in Last 12 Months To</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Employment History</td>
<td>Information regarding prior job experience, positions held, names of prior supervisors, and when permitted by applicable law your salary history or expectations.</td>
<td>B, D, E, F, I, K</td>
</tr>
<tr>
<td>Education Information</td>
<td>Information from resumes regarding educational history; information obtained from transcripts or records of degrees and vocational certifications obtained.</td>
<td>B, D, E, F, I, K</td>
</tr>
<tr>
<td>Professional or Employment-Related Information</td>
<td>Information contained in your personnel file and in other employment documents and records, including information contained in the following types of records: new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury records, safety records, performance evaluations and records, disciplinary records, investigatory records, training records, licensing and certification records, compensation and health benefits records, pension, retirement and 401(k) records, COBRA notifications, business expense records, and payroll records.</td>
<td>A, B, C, D, E, F, G, I, K</td>
</tr>
<tr>
<td>Travel Information</td>
<td>Information regarding business travel, vacation and personal travel plans, and for infectious disease contact tracing purposes the locations travelled to within the applicable infectious period prior to coming to the workplace and the dates spent in those locations.</td>
<td>B, C, D, F, I</td>
</tr>
<tr>
<td>Family Information</td>
<td>Contact information for family members listed as emergency contacts, contact information for dependents and other dependent information, medical and health information for family members related to COVID-19 symptoms, exposure, diagnosis, testing, or vaccination, as well as information related to their travel and whom they have been in close contact with during the applicable COVID-19 infectious period.</td>
<td>B, C, D, F, I</td>
</tr>
<tr>
<td>Information of Friends, Co-workers, and Other Associates with Whom You Have Been in Close Contact within the COVID-19 infectious period per applicable guidelines</td>
<td>Medical and health information provided to the Company for a worksite employee’s friends, co-workers, and other associates related to COVID-19 symptoms, exposure, diagnosis, testing, or vaccination, as well as information related to their travel and whom they have been in close contact with during the applicable COVID-19 infectious period.</td>
<td>B, C, D, F, I</td>
</tr>
<tr>
<td>Medical and Health Information</td>
<td>Medical information contained in such documents as doctor’s notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, ergonomic assessment and accommodation records, and correspondence with you and your medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as information in post-hire drug test results, and information related to COVID-19 symptoms, exposure, contact tracing, diagnosis, testing, or vaccination. This includes medical information and health benefits information for dependents and beneficiaries.</td>
<td>B, C, D, F, I</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td>Disclosed in Last 12 Months To</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Internet, Network, and Computer Activity</td>
<td>Internet or other electronic network activity information related to usage of Company networks, servers, intranet, or shared drives, including system and file access logs, security clearance level, browsing history, search history, and usage history.</td>
<td>B, E, G, I, F, J</td>
</tr>
<tr>
<td>Mobile Device Security Information</td>
<td>Data identifying worksite employee mobile devices accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider.</td>
<td>B, E, G, I, F, J</td>
</tr>
<tr>
<td>Online Portal and Mobile App Access and Usage Information</td>
<td>Username and password, account history, usage history, file access logs, and security clearance level.</td>
<td>B, E, G, I, F, J</td>
</tr>
<tr>
<td>Geolocation Data</td>
<td>IP address and/or GPS location (latitude &amp; longitude) recorded in timekeeping applications that worksite employees use to clock in and out and that log the geographic location at which each time entry was made.</td>
<td>B, E, G, I, F, J</td>
</tr>
<tr>
<td>Systems Access Records</td>
<td>Information identifying which worksite employees accessed secure Company systems and networks and at what times using their login credentials, or other security access method.</td>
<td>B, E, I, F, J</td>
</tr>
</tbody>
</table>

Of the categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect from or about consumers, independent contractors, or applicants:

**Sensitive Personal Information Categories**

<table>
<thead>
<tr>
<th>Personal Identifiers</th>
<th>social security number, driver's license or state identification card number, passport number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Information</td>
<td>your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account</td>
</tr>
<tr>
<td>Protected Classifications</td>
<td>racial or ethnic origin, religious or philosophical beliefs, union membership, or sexual orientation</td>
</tr>
<tr>
<td>Geolocation Data</td>
<td>IP address and/or GPS location, latitude &amp; longitude</td>
</tr>
</tbody>
</table>

**Personal Information DOES NOT include:**

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the worksite employee or from widely distributed media.
- Information made available by a person to whom the worksite employee has disclosed the information if the worksite employee has not restricted the information to a specific audience.
- De-identified or aggregated information.
We may collect your personal information from the following sources:

- You, the worksite employee, when you voluntarily submit information
- Company systems, networks, software applications, and databases you log into or use in the course of performing your job, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Government agencies
- Insurance carriers, administrators, and brokers
- Credit and consumer reporting agencies
- Drug testing and physical testing providers and vendors
- HR support vendors, including administrators of benefits, leaves of absence, workers’ compensation, unemployment claims, payroll, timekeeping, expense management, and training platforms
- Social media platforms
- Recruiters
- Staffing agencies
- Personal references and former worksite employers
- Other worksite employees, contractors, vendors, and customers based on your interactions with them

We may disclose your personal information to the following categories of service providers or third parties:

A. Financial institutions
B. Government agencies
C. Benefits administrators and vendors, including third party administrators, 401K administrators, workers’ compensation and unemployment administrators, insurance brokers, and wellness vendors
D. Insurance carriers, administrators, and brokers
E. Employee tracking and talent management systems
F. Payroll processors, timekeeping vendors, and vendors providing services for purposes of the Company’s human resources information system (HRIS)
G. Communications providers
H. [Intentionally Omitted]
I. Your worksite employer
J. IT and cybersecurity vendors
K. Consumer reporting agencies or credit reporting agencies

By referring to the letter corresponding to the category, the above table specifies to what categories of service providers and third parties we disclose personal information.

We may collect and use your personal information for the following business purposes:

1. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to become a worksite employee, we will use that Personal Information in connection with your employment with your worksite employer or your relationship with us.
2. To assist the Company’s customer (the worksite employer) to comply with local, state, and federal law and regulations requiring maintenance of certain records (such as immigration compliance records, travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records), as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.
3. To comply with local, state, and federal law and regulations that apply to the Company.
4. To manage and process payroll.
5. To validate a worksite employee’s identity for payroll and timekeeping purposes.
6. To maintain commercial insurance policies and coverages, including for workers’ compensation and other liability insurance.
7. To manage workers’ compensation claims.
8. To administer, manage, and maintain group health insurance benefits, 401K and/or retirement plans, and other Company benefits and perks.
9. To provide Human Resources best practices consulting services to the Company’s customer (the worksite employer), including the following topics:
   a. Worksite employer’s management of worksite employees.
   b. Workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct).
   c. Worksite employer’s evaluation of job applicants and candidates for employment or promotions.
   d. Information gathered through background checks on job applicants and worksite employees and to verify employment references.
   e. Worksite employer’s decisions regarding a worksite employee’s employment, including decisions to hire, terminate, promote, demote, transfer, suspend or discipline.
10. To communicate with worksite employees regarding employment-related administrative matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications.
11. To implement, monitor, and manage electronic security measures on Company networks, software applications or systems, including managing and securing online portal CoAdQuantum, CoAdEnroll and CoAd360, as well as on worksite employee devices that are used to access Company networks, software applications or systems.
12. To engage in corporate transactions requiring review or disclosure of worksite employee records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
13. To assist in communications with a worksite employee’s family or other contacts in case of emergency or other necessary circumstance.
14. To assist the Company’s customer (the worksite employer) to promote and foster diversity, equity, and inclusion in the workplace.
15. COVID-19 RELATED PURPOSES – To assist the Company’s customer (the worksite employer) with the following obligations:
   a. To reduce the risk of spreading the disease in or through the workplace.
   b. To protect worksite employees and other consumers from exposure to COVID-19.
   c. To comply with local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19, including applicable reporting requirements.
   d. To facilitate and coordinate pandemic-related initiatives and activities (whether customer-sponsored or through the U.S. Center for Disease Control and Prevention, other federal, state and local governmental authorities, and/or public and private entities or establishments, including vaccination initiatives).
   e. To identify potential symptoms linked to COVID-19 (including through temperature checks, antibody testing, or COVID-19 questionnaire).
f. To permit contact tracing relating to any potential exposure.
g. To communicate with worksite employees and other consumers regarding potential exposure to COVID-19 and properly warn others who have had close contact with an infected or symptomatic individual so that they may take precautionary measures, help prevent further spread of the virus, and obtain treatment, if necessary.

16. To evaluate, assess, and manage the Company’s business relationship with vendors, service providers, and contractors that provide services to the Company.

17. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.

18. To detect security incidents involving potentially unauthorized access to and/or disclosure of Personal Information or other confidential information, including proprietary or trade secret information and third-party information that the Company receives under conditions of confidentiality or subject to privacy rights.

19. To protect against malicious or illegal activity and prosecute those responsible.

20. To prevent identity theft.

21. To verify and respond to consumer requests under applicable consumer privacy laws.

We may disclose your personal information for the following business purposes as numbered above:
1, 2, 3, 4, 5, 6, 7, 8, 9(b), 9(c), 9(d), 9(e), 11, 12, 13, 15(c), 15(f), and 15(g).

We do NOT and will not sell your personal information in exchange for monetary or other valuable consideration. We do not share your personal information for cross-context behavioral advertising.

We do NOT and will not use or disclose your sensitive personal information for purposes other than the following:

1. To perform the services reasonably expected by an average worksite employee who onboards with us.
2. To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
3. To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
4. To ensure the physical safety of natural persons.
5. For short-term, transient use.
6. To perform services on behalf of the Company.
7. To verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company.
8. For purposes that do not involve inferring characteristics about the consumers.
Retention of Personal Information
We will retain each category of personal information seven (7) years after the termination of our service agreement with your worksite employer. In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; contractual requirements, relevant federal, state and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

Third-Party Vendors
We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail and payroll services. Such parties only have access to the personal information needed to perform these functions and may not use or store the information for any other purpose.

Business Transfers
In the event we sell or transfer a particular portion of our business assets, worksite employee information may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, worksite employee information may be transferred as part of the acquisition.

Compliance With Law and Safety
We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect worksite employees or the public.

Passwords
The personal data record created through your registration of your email account for timekeeping and payroll system applications, including mobile applications, can only be accessed with the unique password associated with those records. To protect the integrity of the information contained in those records, you should not disclose or otherwise reveal your passwords to third parties.

Worksite Employees and Their Family Members, Dependents, and Beneficiaries Under the Age of 16
We do not knowingly sell or share the personal information of worksite employees under 16 years of age or any of worksite employee’s family members, dependents or beneficiaries who are under 16 years of age.

How We Protect the Information That We Collect
The protection of the information that we collect about worksite employees is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- We restrict access to private information to those who need such access in the course of their duties for us.
Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents who are natural persons; it does not apply to any entities (whether business, non-profit or governmental). If you are a California resident, you have the following rights:

| Right to Know | The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected, shared or sold about you, (2) the categories of sources from which the personal information was collected, (3) the business purpose for which we use this information, and (4) the categories of third parties with whom we disclose or have disclosed your personal information; |
| Right to Access | The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of personal information we have collected about you; |
| Right to Delete | The right to request, up to 2 times in a 12-month period, that we delete personal information that we have collected from you, subject to certain exceptions; |
| Right to Correct | The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you; |
| Right to Designate | The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and |
| Right to Not be Discriminated or Retaliated Against | The right to not be discriminated or retaliated against for exercising any of the above rights. |

You can submit any of the above types of consumer requests through any of the 2 options below:

<table>
<thead>
<tr>
<th></th>
<th>Submit an online request at: <a href="https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03">https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03</a></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Call our privacy toll-free line at 800-868-1016</td>
</tr>
</tbody>
</table>

How We Will Verify That it is Really You Submitting the Request

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us. For example, we may need you to provide your name, address, email, phone number, last 4 digits of your social security number, and your date of birth.
Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we believe the request is fraudulent.

If You Have an Authorized Agent

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney, or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.
Consent to Terms and Conditions
By onboarding as a worksite employee with CoAdvantage or any of its affiliated companies, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy
As our services evolve and we perceive the need or desirability of using personal information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check CoAdQuantum and/or CoAd360 frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Policy, we will post the revised Policy and the revised effective date on CoAdQuantum and CoAd360. Please check back here periodically or contact us at the address listed at the end of this Policy.

Individuals With Disabilities
This Policy is in a form that is or will be made accessible to individuals with disabilities.

Questions About the Policy
If you have any questions about this Privacy Policy, please contact us at 800-868-1016 or submit a request through https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03

**This Policy was last updated December 31, 2022**
Employee Privacy Policy

CoAdvantage Corporation (the “Company” or “we”) has developed this Privacy Policy out of respect for the privacy of our employees. This Policy describes the personal information we collect, both online and offline, and that we use and disclose about employees who are employed with us. We will collect some information from you for employment purposes.
CoAdvantage CCPA Privacy Policy: Employee

Collection of Personal Information and Sensitive Personal Information

In the last 12 months, we have collected the following categories of personal information from or about employees, including information about employees’ family members, dependents, and beneficiaries. For each category of information, the categories of third parties to whom we have disclosed, sold, or shared the information within the last 12 months are referenced by a letter that coincides with the letter in the list of categories of service providers and third parties that follows soon after this table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Disclosed in Last 12 Months To</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Identifiers</strong></td>
<td>Name, alias, social security number, date of birth, driver's license or state identification card number, passport number, permanent resident alien card number, school ID number, voter’s registration number U.S. military card number, military dependent’s ID card number, U.S. citizen ID card, employee ID number.</td>
<td>A, B, C, D, E, F, H, I</td>
</tr>
<tr>
<td><strong>Contact Information</strong></td>
<td>Home, postal or mailing address, email address, home phone number, cell phone number, emergency contact information.</td>
<td>A, B, C, D, E, F</td>
</tr>
<tr>
<td><strong>Account Information</strong></td>
<td>Username and password for Company accounts and systems, and any required security or access code, password, or credentials allowing access to your Company accounts.</td>
<td>Not Disclosed</td>
</tr>
<tr>
<td><strong>Protected Classifications</strong></td>
<td>Race, ethnicity, national origin, sex, gender, sexual orientation, gender identity, religious or philosophical beliefs, age, disability, medical or mental condition, military status, familial status, or language.</td>
<td>B, C, D, E</td>
</tr>
<tr>
<td><strong>Physical Characteristics or Description</strong></td>
<td>Information on your Driver’s License (such as eye color, hair color, height, weight), as well as information collected to the extent relevant for workplace investigations.</td>
<td>B, C, D</td>
</tr>
<tr>
<td><strong>Biometric Data</strong></td>
<td>Fingerprints</td>
<td>B</td>
</tr>
<tr>
<td><strong>Financial Information</strong></td>
<td>Bank account number for direct deposit, credit card number, debit card number, or other financial account information.</td>
<td>A, B, F</td>
</tr>
<tr>
<td><strong>Pre-Hire Information</strong></td>
<td>Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you.</td>
<td>A, B, D, E, J</td>
</tr>
<tr>
<td><strong>Employment History</strong></td>
<td>Information regarding prior job experience, positions held, names of prior supervisors, and when permitted by applicable law your salary history or expectations.</td>
<td>D, E, J</td>
</tr>
<tr>
<td><strong>Education Information</strong></td>
<td>Information from resumes regarding educational history; information obtained from transcripts or records of degrees and vocational certifications obtained.</td>
<td>D, E, J</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td>Disclosed in Last 12 Months To</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Professional or Employment-Related Information</td>
<td>Information contained in your personnel file and in other employment documents and records, including information contained in the following types of records: new hire or onboarding records, I-9 forms, tax forms, time and attendance records, non-medical leave of absence records, workplace injury records, safety records, performance evaluations and records, disciplinary records, investigatory records, training records, licensing and certification records, compensation and health benefits records, COBRA notifications, business expense records, and payroll records.</td>
<td>A, B, C, D, E, F, J</td>
</tr>
<tr>
<td>Travel Information</td>
<td>Information regarding business travel, vacation and personal travel plans, and for infectious disease contact tracing purposes the locations travelled to within the applicable infectious period prior to coming to the workplace and the dates spent in those locations.</td>
<td>B, D, E</td>
</tr>
<tr>
<td>Family Information</td>
<td>Contact information for family members listed as emergency contacts, contact information for dependents and other dependent information, medical and health information for family members related to COVID-19 symptoms, exposure, diagnosis, testing, or vaccination, as well as information related to their travel and whom they have been in close contact with during the applicable COVID-19 infectious period.</td>
<td>B, D, E</td>
</tr>
<tr>
<td>Information of Friends, Co-workers, and Other Associates with Whom You Have Been in Close Contact within the COVID-19 infectious period per applicable guidelines</td>
<td>Medical and health information provided to the Company for an employee’s friends, co-workers, and other associates related to COVID-19 symptoms, exposure, diagnosis, testing, or vaccination, as well as information related to their travel and whom they have been in close contact with during the applicable COVID-19 infectious period.</td>
<td>B, D, E</td>
</tr>
<tr>
<td>Medical and Health Information</td>
<td>Medical information contained in such documents as doctor’s notes for absences or work restrictions, medical leave of absence records, requests for accommodation, interactive process records, ergonomic assessment and accommodation records, and correspondence with you and your medical or mental health provider(s) regarding any request for accommodation or medical leave of absence, as well as information in post-hire drug test results, and information related to COVID-19 symptoms, exposure, contact tracing, diagnosis, testing, or vaccination. This includes medical information and health benefits information for dependents and beneficiaries.</td>
<td>B, D, E</td>
</tr>
<tr>
<td>Internet, Network, and Computer Activity</td>
<td>Internet or other electronic network activity information related to usage of Company networks, servers, intranet, shared drives, or Company-issued computers and electronic devices, including system and file access logs, browsing history, search history, and usage history</td>
<td>E, G</td>
</tr>
<tr>
<td>Mobile Device Security Information</td>
<td>Data identifying employee’s devices accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider</td>
<td>D, E, G</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td>Disclosed in Last 12 Months To</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Online Portal and Mobile App Access and Usage Information</td>
<td>Username and password, account history, usage history, file access logs.</td>
<td>D, E, G</td>
</tr>
<tr>
<td>Geolocation Data</td>
<td>IP address and/or GPS location (latitude &amp; longitude) recorded on Company-issued computers, and electronic devices,</td>
<td>D, E, G</td>
</tr>
<tr>
<td>Visual, Audio or Video Recordings in the Workplace</td>
<td>Your image when recorded or captured in surveillance camera footage or pictures of employees taken in the workplace or at a Company function or event, or in pictures or video of employees posted on social media to which the Company or its managers have access or that are submitted to the Company by another employee or third party.</td>
<td>B, D, E, H, I</td>
</tr>
<tr>
<td>Facility &amp; Systems Access Records</td>
<td>Information identifying which employees accessed secure Company facilities, systems, networks, computers, and equipment and at what times using their keys, badges, fobs, login credentials, or other security access method.</td>
<td>B, D, E</td>
</tr>
<tr>
<td>Inferences</td>
<td>Based on analysis of the personal information collected, we may develop inferences regarding behavioral traits.</td>
<td>Not Disclosed</td>
</tr>
<tr>
<td>Contents of Personal Communications where the Company is not the intended recipient</td>
<td>If you use Company email, phones, computers, online chat applications (Slack, Teams, Zoom, etc.) or other Company systems for personal communications where the Company is not the intended recipient of the communication, the Company retains these communications in the ordinary course of managing its communication and computer systems and pursuant to the Company’s data retention policy. Employees have no expectation of privacy with respect to any communications or data they send, receive, access or store on any company computer or system, including any personal communications. The Company may monitor, access, review and use all such communications and data for lawful business purposes detailed below, including to manage and evaluate employee performance and make employment decisions.</td>
<td>Not Disclosed</td>
</tr>
</tbody>
</table>
Of the categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect from or about consumers, independent contractors, or applicants:

### Sensitive Personal Information Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Identifiers</strong></td>
<td>social security number, driver’s license or state identification card number, passport number</td>
</tr>
<tr>
<td><strong>Account Information</strong></td>
<td>your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account</td>
</tr>
<tr>
<td><strong>Protected Classifications</strong></td>
<td>racial or ethnic origin, religious or philosophical beliefs, union membership, or sexual orientation</td>
</tr>
<tr>
<td><strong>Biometric Information</strong></td>
<td>Used for the purpose of uniquely identifying you</td>
</tr>
<tr>
<td><strong>Medical and Health Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Geolocation Data</strong></td>
<td>IP address and/or GPS location, latitude &amp; longitude</td>
</tr>
<tr>
<td><strong>Contents of Personal Communications</strong></td>
<td>contents of mail, email, and text messages where the Company is not the intended recipient</td>
</tr>
</tbody>
</table>

**Personal Information DOES NOT include:**

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the employee or from widely distributed media.
- Information made available by a person to whom the employee has disclosed the information if the employee has not restricted the information to a specific audience.
- De-identified or aggregated information.

We may collect your personal information from the following sources:

- You, the employee, when you voluntarily submit information for employment purposes
- Company-issued computers, and electronic devices.
- Company systems, networks, software applications, and databases you log into or use in the course of performing your job, including from vendors the Company engages to manage or host such systems, networks, applications or databases
- Surveillance cameras at our physical locations
- Credit and consumer reporting agencies
- Drug testing and physical testing providers and vendors
- HR support vendors, including administrators of benefits, workers’ compensation, unemployment claims, payroll, timekeeping, expense management
- Social media platforms
- Recruiters
- Staffing agencies
- Personal references and former employers
- Our other employees, contractors, vendors, suppliers, guests, visitors, and customers based on your interactions with them
We may disclose your personal information to the following categories of service providers or third parties:

A. Financial Institutions
B. Government Agencies
C. Benefits Administrators and Insurers, including health and welfare, 401k, workers’ compensation and unemployment administrators or vendors
D. Employee Tracking and Talent Management Systems
E. Professional Employer Organizations
F. Payroll Processors
G. Communications Providers
H. Social Media Platforms
I. Our Corporate Customers
J. Consumer reporting agencies or credit reporting agencies

By referring to the letter corresponding to the category, the above table specifies to what categories of service providers and third parties we disclose personal information.

We may collect and use your personal information for the following business purposes:

1. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to become an employee, we will use that Personal Information in connection with your employment.
2. To comply with local, state, and federal law and regulations requiring employers to maintain certain records (such as immigration compliance records, travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records), as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.
3. To manage and process payroll and/or Company travel and expenses.
4. To validate an employee’s identity for payroll and timekeeping purposes.
5. To maintain commercial insurance policies and coverages, including for workers’ compensation and other liability insurance.
6. To manage workers’ compensation claims.
7. To administer, manage, and maintain group health insurance benefits, 401K and/or retirement plans, and other Company benefits and perks.
8. To manage employee performance of their job duties and/or employee conduct, including by engaging in lawful monitoring of employee activities and communications when they are on duty, on Company premises, working remotely per the terms of the Company policy, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
9. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment, or other misconduct).
10. To evaluate job applicants and candidates for employment or promotions.
11. To obtain and verify background checks on job applicants and employees and to verify employment references.
12. To evaluate, make, and communicate decisions regarding an employee’s employment, including decisions to hire, terminate, promote, demote, transfer, suspend or discipline.
13. To communicate with employees regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W2s, and other alerts and notifications.
14. To grant employees access to secure Company facilities and maintain information on who accessed the facility.
15. To track employee movement and activity throughout Company facilities and keep the facilities secure.
16. To implement, monitor, and manage electronic security measures on Company internet and WiFi connections, computers, networks, devices, software applications or systems, as well as on employee devices that are used to access Company internet and WiFi connections, computers, networks, devices, software applications or systems.
17. To engage in corporate transactions requiring review or disclosure of employee records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
18. To communicate with an employee’s family or other contacts in case of emergency or other necessary circumstance.
19. To manage employee recognition programs.
20. To promote and foster diversity, equity, and inclusion in the workplace.
21. To provide services to corporate customers who may request certain pieces of information about a Company employee (such as name, phone number, and headshot) to permit the employee access or security clearance to their facility in advance of the Company employee being dispatched to provide services at the customer’s facility.

22. COVID-19 RELATED PURPOSES
   a. To reduce the risk of spreading the disease in or through the workplace.
   b. To protect employees and anyone who interacts with our employees from exposure to COVID-19.
   c. To comply with local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19, including applicable reporting requirements.
   d. To facilitate and coordinate pandemic-related initiatives and activities (whether Company-sponsored or through the U.S. Center for Disease Control and Prevention, other federal, state and local governmental authorities, and/or public and private entities or establishments, including vaccination initiatives).
   e. To identify potential symptoms linked to COVID-19 (including through temperature checks, antibody testing, or COVID-19 questionnaire).
   f. To permit contact tracing relating to any potential exposure.
   g. To communicate with employees and others who interacted with our employees regarding potential exposure to COVID-19 and properly warn others who have had close contact with an infected or symptomatic individual so that they may take precautionary measures, help prevent further spread of the virus, and obtain treatment, if necessary.

23. To evaluate, assess, and manage the Company’s business relationship with vendors, service providers, and contractors that provide services to the Company.
24. To improve user experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
25. To detect security incidents involving potentially unauthorized access to and/or disclosure of Personal Information or other confidential information, including proprietary or trade secret information and third-party information that the Company receives under conditions of confidentiality or subject to privacy rights.
26. To protect against malicious or illegal activity and prosecute those responsible.
27. To prevent identity theft.
28. To verify and respond to consumer requests under applicable consumer privacy laws.
We may disclose your personal information for the following business purposes as numbered above:
1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 16, 17, 18, 21, 22(c), 22(f) and 22(g).

We do NOT and will not sell your personal information in exchange for monetary or other valuable consideration. We do not share your personal information for cross-context behavioral advertising.

We do NOT and will not use or disclose your sensitive personal information for purposes other than the following:

1. To perform the services reasonably expected by an average employee who requests those services.
2. To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
3. To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
4. To ensure the physical safety of natural persons.
5. For short-term, transient use.
6. To perform services on behalf of the Company.
7. To verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company.
8. For purposes that do not involve inferring characteristics about the consumers.
Retention of Personal Information
We will retain each category of personal information for seven (7) years after termination of employment. In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statute of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

Third-Party Vendors
We may use other companies and individuals to perform certain functions on our behalf. Examples include administering e-mail and payroll services. Such parties only have access to the personal information needed to perform these functions and may not use or store the information for any other purpose.

Business Transfers
In the event we sell or transfer a particular portion of our business assets, employee information may be one of the business assets transferred as part of the transaction. If substantially all of our assets are acquired, employee information may be transferred as part of the acquisition.

Compliance With Law and Safety
We may disclose specific personal and/or sensitive personal information based on a good faith belief that such disclosure is necessary to comply with or conform to the law or that such disclosure is necessary to protect our employees or the public.

Passwords
The personal data record created through your registration for your employee email account and timekeeping and payroll system applications including through use of CoAdQuantum, CoAdEnroll and CoAd360, can only be accessed with the unique password associated with those records. To protect the integrity of the information contained in those records, you should not disclose or otherwise reveal your passwords to third parties.

Employees and Their Family Members, Dependents, and Beneficiaries Under the Age of 16
We do not knowingly sell or share the personal information of employees or any of their family members, dependents or beneficiaries under 16 years of age.

How We Protect the Information That We Collect
The protection of the information that we collect about employees is of the utmost importance to us and we take every reasonable measure to ensure that protection, including:

- We use commercially reasonable tools and techniques to protect against unauthorized access to our systems.
- We restrict access to private information to those who need such access in the course of their duties for us.
Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents who are natural persons; it does not apply to any entities (whether business, non-profit or governmental). If you are a California resident, you have the following rights:

| Right to Know | The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected, shared or sold about you, (2) the categories of sources from which the personal information was collected, (3) the business purpose for which we use this information, and (4) the categories of third parties with whom we disclose or have disclosed your personal information; |
| Right to Access | The right to request, up to 2 times in a 12-month period, that we provide you access to or disclose to you the specific pieces of personal information we have collected about you; |
| Right to Delete | The right to request, up to 2 times in a 12-month period, that we delete personal information that we have collected from you, subject to certain exceptions; |
| Right to Correct | The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you; |
| Right to Designate | The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and |
| Right to Not be Discriminated or Retaliated Against | The right to not be discriminated or retaliated against for exercising any of the above rights. |

You can submit any of the above types of consumer requests through any of the 3 options below:

Submit an online request at: [https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03](https://coadvantage-privacy.my.onetrust.com/webform/8e2657c7-e21d-49f1-aa35-a7e73d91571a/22f9a25f-10a7-4fb6-b47e-e231dd536b03)

Call our privacy toll-free line at 941-925-2990

Complete a paper form, which can be requested at any of the following locations:
- 18301 Von Karman Blvd., Ste. 490, Irvine, CA 92614
- 35 N. Lake Avenue, Ste. 140, Pasadena, CA 91101
- 12526 High Bluff Drive, Ste. 230, San Diego, CA 92130.

How We Will Verify That it is Really You Submitting the Request

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular information in our possession, which depends on the nature of your relationship and interaction with us. For example, we may need you to provide your name, address, email, phone number, last 4 digits of your social security number, and your date of birth.
Responding to your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessarily information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we believe the request is fraudulent.

If You Have an Authorized Agent

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power of attorney, or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf. We will also contact you and ask you for information to verify your own identity directly and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.
Consent to Terms and Conditions
By entering into an employment relationship with CoAdvantage Corporation, you consent to all terms and conditions expressed in this Privacy Policy.

Changes to Our Privacy Policy
As our services evolve and we perceive the need or desirability of using personal information collected in other ways, we may from time to time amend this Privacy Policy. We encourage you to check CoAdQuantum or CoAd360 frequently to see the current Privacy Policy in effect and any changes that may have been made to them. If we make material changes to this Policy, we will post the revised Policy and the revised effective date on CoAdQuantum and CoAd360. Please check back here periodically or contact us at the address listed at the end of this Policy.

*This Policy was last reviewed in January 2024.

Individuals With Disabilities
This Policy is in a form that is or will be made accessible to individuals with disabilities.

Questions About the Policy
If you have any questions about this Privacy Policy, please contact us at:

- #Dept-InternalHR@coadvantage.com,
- or