PRIVACY NOTICE

Employees, Contractors & Job Applicants

Last Updated: December 22, 2022

As an employee, contractor or job applicant, you have the right to know what categories of personal information Omron Management Center of America, Inc. and its affiliates ("Omron") collect about you and the purposes for which such information is collected by Omron.

As used in this Privacy Notice, "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. Personal information includes, but is not limited to, the categories of personal information identified below if such information identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household ("Personal Information").

Personal information may be collected by Omron directly from employees, contractors or job applicants, by a service provider used by Omron or other publicly accessible source (e.g. an online profile).

If you want to exercise your privacy rights, please submit your request through this web form.

Categories of Personal Information Collected

EMPLOYEES & CONTRACTORS (CURRENT AND FORMER)

- Identifiers, such as a real name, alias, postal home address, unique personal identifier, online identifier, email address, phone number, age, gender, marital status, family member/beneficiary related information, emergency contact information, employee number, account name, social security number, social security card copy, driver's license number, passport number, a photo ID copy or other similar identifiers.
- Health insurance information, including an individual's insurance policy number or subscriber identification number and individual's dependent names and any unique identifier used by a health insurer to identify the individual, or any information in the individual's application and claims history
- Medical information, including any information in possession of or derived from a healthcare provider, healthcare service plan, pharmaceutical company, or contractor regarding an individual's medical history, mental or physical condition, or treatment.
- Financial information, including bank account number, credit card number, debt/loan, child or spousal support information disclosed in wage garnishment subpoenas or other financial information.
- Characteristics of protected classifications under state or federal law, such as race, gender, physical or mental disability, religion and military status.
- Intellectual Property information related to you, including filings and descriptions of IP, projects or other related work.
- Biometric information
- Audio, electronic, visual, thermal, olfactory, or similar information (*e.g.*, an employee profile photograph, product demonstration video or recording of a customer service call).
- Internet or other electronic network activity information, such as browsing history, search history, and information regarding an individual's interaction with an internet website, application, or advertisement.
- Geolocation data. This category includes GPS location data from Firm-issued mobile devices and Firm-owned vehicles.

- Professional or employment-related information.
- Education information or other academic information.
- Written signatures.
- Inferences drawn from or compilation of any of the information listed above.

JOB APPLICANTS

Categories of Personal Information Collected

- Identifiers, such as a first name, middle name, last name, alias, postal home address, unique personal identifier, online identifier, email address, phone number, account name, passwords, social security number, driver's license number, photo ID copy or other similar identifiers;
- Work authorization status;
- CV, resume, cover letter, professional or employment-related information and education information or other academic information;
- Knowledge, skills and abilities;
- Professional and other work-related licenses, permits, and certifications held;
- Referral names and contact information for referrals;
- Assessment information and materials provided during the applicant evaluation process (e.g. test, surveys, case studies and work samples);
- Written signatures;
- Information relating to character and employment references;
- Characteristics of protected classifications under state or federal law, such as race, gender, physical or mental disability, religion and military status; and
- Any other information you elect to provide to us (e.g. employment preferences, willingness to relocate, current salary, desired work salary, awards, or professional memberships).

Purpose of the collection of Personal Information

EMPLOYEES AND CONTRACTORS (CURRENT AND FORMER)

- Manage your employment or contractor relationship with us.
- Compensation, work-related travel and expense reimbursement, payroll, tax, and benefits planning, enrollment, and administration.
- Perform background checks and verify past employment, educational history, and professional standing and qualifications.
- Provide you access to Omron systems, networks, databases, equipment, and facilities.
- Workforce development, education, training, and certification.
- Monitor, maintain, and secure Omron systems, networks, databases, equipment, and facilities.
- Authenticate your identity and verify your access permissions.
- Arrange, confirm, and monitor work-related travel, events, meetings, and other activities.
- Contact and communicate with you regarding your employment, job performance, compensation, and benefits, or in the event of a natural disaster or other emergency.
- Contact and communicate with your designated emergency contacts in the event of an emergency, illness, or absence.
- Contact and communicate with your dependents and designated beneficiaries in the event of an emergency or in connection with your benefits.
- Create internal communications such as e-mails and newsletters.
- Provide benefit planning and coverage.
- Communicate with you or your healthcare/benefit providers in connection with your benefits.
- Assess your working capacity or the diagnosis, treatment or care of a condition impacting your fitness for work, and other preventative or occupational medical purposes (including work-related injury and illness reporting).

- Comply with court orders.
- Comply with laws and regulations including tax and anti- discrimination laws.
- Create materials for internal communications such as e-mails and newsletters.
- Review any potential conflicts of interest.
- Authenticate your identity for attendance tracking.
- Authenticate your identity and verify your access permissions.
- Identify you in Omron systems, networks, databases, equipment, and facilities (e.g. on ID badges, employee directory, etc.)
- Create material used for business purposes (e.g. promotional videos, newsletters, internal communications, etc.)
- Workforce and performance management, including personnel planning, productivity monitoring, and evaluation.
- Monitor, maintain, and secure Omron systems, networks, databases, equipment, and facilities.
- Improve safety of employees, customers and the public with regard to use of Omron property and equipment
- Preventing unauthorized access, use, or loss of Omron property
- Improve efficiency, logistics, and supply chain management
- Ensuring employee productivity and adherence to Omron's policies
- Investigate complaints, grievances, and suspected violations of Omron policy

JOB APPLICANTS

- Evaluating a potential employment or contractor relationship with you;
- Assessing your skills, qualifications, and interests against our career opportunities;
- Verifying your personal information, past employment, educational history and professional qualifications;
- Carrying out reference checks and/or conducting background checks (where applicable) if you are offered a job;
- Evaluating and determining your compensation, payroll, and benefits;
- Contacting you regarding your application and potential employment relationship with Omron;
- Creating a profile about an individual reflecting the individual's characteristics, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Complying with applicable laws, regulations, legal processes, or enforceable governmental requests, including (without limitation) applicable tax, health and safety, anti-discrimination, immigration, labor and employment, and social welfare laws; and/or
- Entering into various confidentiality agreements and other pre-employment or employment documents and agreements.
- Monitoring, investigating, and enforcing compliance with and potential breaches of Omron policies and procedures and legal and regulatory requirements.
- Complying with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons.
- Exercising or defending the legal rights of Omron and its employees, affiliates, customers, contractors, and agents.

If you are offered and accept employment with Omron, the personal information collected during the job application and recruitment process may become part of your employment record.

You will not be subject to hiring decisions based solely on automated data processing without your prior consent.

Disclosures of Data

In addition to the purposes identified above, Omron may use and disclose any and all personal information that we collect to our affiliates, service providers or third party as necessary or appropriate to:

- Comply with laws and regulations, including (without limitation) applicable tax, health and safety, anti-discrimination, immigration, labor and employment, and social welfare laws.

- Monitor, investigate, and enforce compliance with and potential breaches of Omron policies and procedures and legal and regulatory requirements.
- Comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons.
- Exercise or defend the legal rights of Omron and its employees, affiliates, customers, contractors, and agents.

Security of My Personal Information

We have implemented reasonable precautions to protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please be aware that despite our efforts, no data security measures can guarantee security completely. Although we do our best to protect your information, we cannot guarantee the security of your personal information transmitted through our Services, including our mobile applications. Further, we are not responsible for circumvention of any privacy settings or security measure we provide. Please take steps to protect against unauthorized access to your password, phone, mobile device, or computer by, among other things, signing off after using a shared computer or device, choosing a robust password that nobody else knows or can easily guess, and keeping your log-in and password private. We are not responsible for any lost, stolen, or compromised passwords or for any activity on your account via unauthorized password activity.

Data Retention

We keep your personal information only for so long as necessary to fulfill the purposes for which it was collected and for other legitimate business purposes, including to meet our legal, regulatory, or other compliance obligations. Omron will retain your information indefinitely if it believes in good faith that we have a legal obligation to do so.

California Privacy Rights

Pursuant to the California Consumer Privacy Act ("CCPA") and the California Privacy Rights Act ("CPRA"), Omron is required to inform California residents who are employees, contractors, or job applicant about the categories of Personal Information ("Personal Information") and Sensitive Personal Information ("Sensitive Personal Information") we collect or have collected in the past 12 months and the purposes for which we use this information. Omron is committed to protecting the privacy and security of Personal Information and Sensitive Personal Information of all individuals.

This Notice of Collection ("Notice") explains what types of Personal Information and Sensitive Personal Information we may collect about our employees, contractors, or job applicants in the ordinary course of business and how that Personal Information and Sensitive Personal Information may be used. This Notice is to be provided at or before the point of collection of Personal Information and Sensitive Personal Information. In this Notice, the terms "we," "us," and "our" refer to Omron. This Notice contains disclosures required by the CCPA and CPRA, and pertains only to the Personal Information and Sensitive Personal Information that we may have collected within the preceding 12 months or may collect about a California resident in the course of such person acting as an employee of, director of, officer of, contractor, or job applicant of Omron, or job applicants (to the extent that such person's Personal Information or Sensitive Personal Information is or was collected and used by Omron solely within the context of the person's role or former role as an employee of, director of, officer of, a contractor or job applicant of Omron).

In the preceding 12 months, we have collected the categories of Personal Information and Sensitive Personal Information set forth in the table below. The purposes may vary according to whether you are a job applicant, or an employee or contractor of Omron, please refer to the Use of Information section above for the purposes. In the preceding 12 months, we have disclosed the following categories of Personal Information to the following categories of recipients:

Category of Personal Information	***Examples***	***Collected***	***Disclosed for a business purpose within the past 12 months?***	***Sold or Shared with Third Parties within the past 12 months?***	***Categories of Recipients***
Identifiers	Name, alias, address, email address, IP address, account name, unique device ID, etc	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firms, etc.
Personal Information listed in California Customer Records Statute (Cal. Civ. Code §1798.80(e)) *Note: Some personal information included in this category may overlap with other categories*	Name, signature, address, telephone number, state ID number, financial information, medical information, etc.	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm, etc.
Protected classifications characteristics	Gender, age, marital status, etc.	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Commercial information	Information about Services purchased, obtained, or considered	No	No	No	Not applicable
Biometric information	Facial recognition, sleep data, health data, fingerprint, etc	No	No	No	Not applicable
Internet or other similar network, browsing, or search activity	Domain information, browsing activity, session information, cookie information	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers,

					information technology, cloud service, law firm etc.
Geolocation information	Physical location or movements	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Sensory information	Audio, electronic, visual, thermal, olfactory, or similar information.	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Professional or employment-related information	Current or past job history or performance evaluations.	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Non-publicly available educational information under the Family Educational Rights and Privacy act (FERPA) and related regulations	Education records directly related to a student maintained by an educational intuition or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	No	No	No	Not applicable
Inferences drawn from other personal information to create consumer profiles.	Characteristics, interests, and trends	No	No	No	Not applicable

CPRA has required us to disclose the collection of your sensitive personal information. In the preceding 12 months, we have collected the following categories of sensitive personal information set forth below and we have disclosed the following categories of sensitive personal information to the following categories of recipients.

Category of Sensitive Personal Information	***Examples***	***Collected***	***Disclosed for a business purpose within the past 12 months?***	***Sold or Shared with Third Parties within the past 12 months?***	***Categories of Recipients***
Government Identifiers	social security, driver's license, state identification card, or passport number	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Complete account access credentials	User names, account numbers, or card numbers combined with required access/security code or password	No	No	No	Not applicable
Precise geolocation	Physical location or movements	No	No	No	Not applicable
Racial or ethnic origin	-	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Religious or philosophical beliefs	-	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Union membership	-	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.
Genetic data	-	No	No	No	N/A
Mail, email, or text message contents	The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers,

					information technology, cloud service, law firm etc.
Unique identifying biometric information	-	No	No	No	N/A
Medical information	Health information (such as blood pressure readings, sleep data , health related information, sex life, or sexual orientation information)	Yes	Yes	No	Affiliates. Vendors and service providers such as ADP, Vitality, insurance carriers, information technology, cloud service, law firm etc.

Do Not Sell or Share My Personal Information
Omron collects does not sell or otherwise disclose your Personal Information to any third parties for monetary consideration. Omron only shares your Personal Information or Sensitive Personal Information with service providers to the extent necessary to administer employee benefits, including payment of wages, tax processing, and health insurance and in connection with its human resources activities. Omron also discloses your Personal Information or Sensitive Personal Information when required to be in compliance with applicable local, state or federal law.

Updating and Accessing Your Personal Data
You must promptly inform us when changes occur in the Personal Information or Sensitive Personal Information you have provided so that we can maintain accurate Personal Information and Sensitive Personal Information about you. Although you may update or change your Information, we may maintain such Personal Information and Sensitive Personal Information previously submitted in historical archives.

Your Rights under the CCPA and CPRA
Subject to certain limitations, you have the right to:

- request to know more about the categories and specific pieces of personal information we collect, use, disclose, and sell,
- request deletion of your personal information,
- request to correct inaccuracies of your personal information
- opt out of any "sales" or "sharing" of your personal information that may be occurring,
- limit the use and sharing of sensitive personal information
- opt out of automated decision-making
- request to have your personal information transmitted to another entities ("Data portability"), and
- not be discriminated against for exercising these rights.

The privacy rights request is subject to our being able to reasonably verify your identity and authority to make these requests. In order to verify your identity when you submit a request, we will ask you to provide two (2) or three (3) pieces of personal information to confirm in our records. For example, if you purchased an Omron product or Service through our Site, you will be asked to provide at least your name and details of your recent interactions with us.

How to Submit a Request Under the CCPA or CPRA. If your Personal Information is subject to the CCPA or CPRA, you may make these requests by calling 1 (833) 625 1108 or completing this web form. You may also authorize someone to exercise these rights on your behalf. In order to do so, we require signed permission. If we receive your request from an authorized agent, we may ask for evidence that you have provided such agent with power of attorney or equivalent document that the agent otherwise has valid written authority to submit requests to exercise rights on your behalf. We will not discriminate against you if you exercise your rights under the CCPA or CPRA.

If we receive your request from an authorized agent, we may ask for evidence that you have provided such agent with a power of attorney or that the agent otherwise has valid written authority to submit requests to exercise rights on your behalf. Once we have a copy of the valid signed authorization, your designated representative/authorized agent will be able to exercise these rights with respect to the account(s) listed on such authorization for the life of the account, unless there is a specified term or expiration date on the authorization form. Any information gathered as part of the verification process will be used for verification purposes only. Responses to verifiable consumer requests will be delivered through secure email or postal mail, depending on your election when you submit such requests.

Authorized Agents. You may use an authorized agent to submit a rights request. If you do so, the authorized agent must present signed written authorization to act on your behalf, and you will also be required to independently

verify your own identity directly with us and confirm with us that you provided the authorized agent permission to submit the rights request. This verification process is not necessary if your authorized agent provides documentation reflecting that the authorized agent has power of attorney to act on your behalf under Cal. Prob. Code §§ 4121 to 413. If you are an authorized agent seeking to make a request, please contact us by phone at 1 (833) 625 1108 or online by completing this web form.

Aggregated and Deidentified Personal Information

Omron does share and disclose aggregated and deidentified personal information from our health insurance carrier to third party, such data is exempt from the CCPA to third parties. To aggregate and deidentify the personal information, we followed the HIPAA safe harbor method to remove the identifiers.

Canada Privacy Rights

Data Sharing

We will only disclose your personal information to third parties where required by law or to our employees, contractors, designated agents, or third-party service providers who require it to assist us with administering the employment relationship with you or for the recruiting process. Third-party service providers include, but are not limited to, payroll processors and benefits administration providers. These third-party service providers may be located outside of Canada.

We require all our third-party service providers, by written contract, to implement appropriate security measures to protect your personal information consistent with our policies and any data security obligations applicable to us as your employer. We do not permit our third-party 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.

We may also disclose your personal information for the following additional purposes where permitted or required by applicable law:

- To other members of our group of companies (including outside of Canada) for the purposes set out in this Privacy Policy and as necessary to perform our employment contract with you.
- As part of our regular reporting activities to other members of our group of companies.
- To comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders. When we disclose your personal information to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal information necessary for the specific purpose and circumstances.
- During emergency situations or where necessary to protect the safety of persons.
- Where the personal information is publicly available.
- If a business transfer or change in ownership occurs.
- For additional purposes with your consent where such consent is required by law.

Cross-Border Data Transfers

Where applicable law permits, we may transfer the personal information we collect about you to the United States and other jurisdictions that may not be deemed to provide the same level of privacy protection as Canada, as necessary to perform our employment contract with you and for the purposes set out in this Privacy Policy.

The measures that we use to protect personal information are subject to the legal requirements of the jurisdictions to which we transfer personal information, including lawful requirements to disclose information to law enforcement and government agencies in those countries.

Rights of Access, Correction, Erasure, and Objection

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your employment. By law you have the right to request access to and to correct the personal information that we hold about you, or withdraw your consent to the use of your personal information under certain circumstances. If you want to review, verify, correct, or withdraw consent to the use of your personal information, please submit your request by completing this web form.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal information that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal information that we hold about you, or we may have destroyed, erased, or made your personal information anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Changes to Notice

This Notice is reviewed and updated annually to ensure it accurately captures our practices and procedures. Omron may add to the categories of Personal Information it collects and the purposes for which it uses that Personal Information. In that case, Omron will inform you.

Contact Us

If you have questions about our privacy policies and procedures, you may contact OMCA HR or OMCA Legal