SNAP-ON INCORPORATED
CALIFORNIA WORKFORCE PRIVACY NOTICE

This privacy notice answers frequently asked questions about the kinds of Personal Information the Snap-on Incorporated group of companies (referred to as "**Snap-on Group**" or "**we**") collect from you and how it is used, disclosed and retained.

This notice covers Personal Information pertaining to California residents that are applicants, employees, owners, directors, officers, medical staff members, contractors, and any of their emergency contacts, and any of their employment benefits beneficiaries. This notice would not cover Personal Information related to the purchase of any products or services from Snap-on.

The protection of your Personal Information is an important concern to which we pay special attention.

Should you have any questions or concerns regarding this privacy notice, please contact the data protection manager at: DataProtectionManager@snapon.com.

Notice At Collection

1. What types of Personal Information do we gather?

We may collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household ("**Personal Information**").

Personal Information does not include:

- Publicly available information from government records or widely distributed media.
- Deidentified or aggregated information.
- Information excluded from the CCPA's scope, like: health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the California Confidentiality of Medical Information Act (CMIA); and personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

In particular, we may collect and process a range of Personal Information including the following categories, and we may disclose it for our business and operational purposes to the following categories of entities. This table also reflects our collection and disclosure of Personal Information over the last 12 months:

Category	Examples (not all inclusive)	Disclosed to Which Categories of Third Parties for Operational or Business Purposes
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address if linked to an individual, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Our affiliates; Service providers that provide services such as payroll, health & various welfare benefits, retirement saving & equity benefits, background and employment screening services, security management, legal and professional consulting, training, expense management, IT, and other services; professional advisors, such as accountants, auditors, bankers, and lawyers; public and governmental authorities and agencies, such as regulatory authorities and law enforcement; third parties in response to subpoenas.
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Our affiliates; Service providers that provide services such as payroll, health & various welfare benefits, retirement saving & equity benefits, background and employment screening services, security management, legal and professional consulting, training, expense management, IT, and other services; professional advisors, such as accountants, auditors, bankers, and lawyers; public and governmental authorities and agencies, such as regulatory authorities and law enforcement; third parties in response to subpoenas.

C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	Our affiliates; Service providers that provide services such as payroll, health & various welfare benefits, retirement saving & equity benefits, background and employment screening services, security management, legal and professional consulting, training, expense management, IT, and other services; professional advisors, such as accountants, auditors, bankers, and lawyers; public and governmental authorities and agencies; third parties in response to subpoenas.
D. Biometric information.	An individual's physiological, biological or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity.	Professional advisors, such as accountants, auditors, bankers, and lawyers; third parties in response to subpoenas.
E. Internet or other similar network activity.	Browsing history, search history, information on your interaction with a website, application, or Snap-on equipment.	Service providers that provide services such as payroll, benefits, consulting, training, expense management, medical/health, IT, and other services; professional advisors, such as accountants, auditors, bankers, and lawyers; third parties in response to subpoenas.
F. Geolocation data.	Physical location or movements.	Service providers that provide services such as time and attendance, payroll, security management and other services; professional advisors, such as accountants, auditors, bankers, and lawyers; third parties in response to subpoenas.
G. Sensory data.	Audio, electronic, or similar information.	Third parties in response to subpoenas.

H. Professional or employment-related information.	Current or past job history, resume and employment application information, background checks, information necessary to administer employee benefits for employees and the beneficiaries of their employment benefits, information from income tax forms, information about emergency contacts, performance evaluations.	Our affiliates; Service providers that provide services such as payroll, health & various welfare benefits, retirement saving & equity benefits, background and employment screening services, security management, legal and professional consulting, training, expense management, IT, and other services; professional advisors, such as accountants, auditors, bankers, and lawyers; public and governmental authorities and agencies; third parties in response to subpoenas.
I. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists.	Not disclosed.
J. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Service providers that provide services such as health and various welfare benefits, legal and professional consulting; professional advisors, such as accountants, auditors, bankers, and lawyers; public and governmental authorities and agencies including law enforcement; third parties in response to subpoenas.
Sensitive Personal Information • Personal Information that reveals an individual's Social Security, driver's license, state identification card, or passport		Third parties in response to subpoenas.

number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;		

2. How is that Personal Information used by us?

We may use your Personal Information in the following ways:

- **Business Uses, such as:**
  - to evaluate an employment application;
  - determining eligibility for employment;
  - providing access to, and ensuring the security of company physical facilities;
  - administering pay, expenses, and benefits;
  - administering employee recognition and reward schemes;
  - processing employee work-related claims;
  - establishing training and/or development requirements;
  - conducting performance and goal reviews;
  - assessing qualifications for a job or task;
  - gathering evidence for disciplinary action or termination;
  - establishing a contact in the event of an emergency;
  - establishing beneficiaries and administering their benefits;
  - reporting on company metrics;
  - compiling directories;
  - complying with applicable labor or employment statutes;
  - arranging travel;
  - administering company credit cards;
  - conducting fleet management;
  - providing access, monitoring and supporting the use, and ensuring the security of IT systems and company-held information and assets; and
  - other purposes as are reasonably required by the Snap-on Group based on the context of your relationship.

3. How is Sensitive Personal Information used by us?

We collect, use, and disclose Sensitive Personal Information for purposes of ensuring the security and integrity of our business, services, infrastructure, and the individuals we interact with, establishing and maintaining your employment relationship with us, ensuring the diversity of our workforce, complying with legal obligations, managing payroll and corporate credit card use, administering and providing benefits, securing the access to, and use of, our facilities, equipment, systems, networks, applications and infrastructure, preventing, detecting, and investigating security incidents, resisting and responding to fraud or illegal activities, ensuring the physical safety of individuals, and other collection and processing that is not for the purpose of inferring characteristics about an individual. We do not use or disclose Sensitive Personal Information for additional purposes.

4. For what purposes do we disclose Personal Information?

We disclose Personal Information to our service providers and providers of the benefits we offer to our employees to enable them to provide services to us and to provide benefits to our employees and their beneficiaries. We also disclose Personal Information to service providers to perform background checks and at the request of our personnel and former personnel, for example to provide employment verification to third parties.

We may disclose Personal Information to any member of our group, which means our subsidiaries, or our ultimate holding company and its subsidiaries, to enable them to provide services to the Snap-on Group.

We may also disclose Personal Information to a third party in the context of any reorganization, financing transaction, merger, sale, joint venture, partnership, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

We do not sell Personal Information (including Sensitive Personal Information), and we do not "share" Personal Information (including Sensitive Personal Information) for purposes of cross-context behavioral advertising, as defined under the CCPA. We have not engaged in such activities in the 12 months preceding the date this Policy was last updated. Without limiting the foregoing, we do not sell or "share" Personal Information (including Sensitive Personal Information) of minors under 16 years of age and have no actual knowledge of any such sale or "sharing."

5. Retention of Personal Information

We retain each category of Personal Information, including Sensitive Personal Information, for as long as needed or permitted in light of the purpose(s) for which it was collected. The criteria used to determine our retention periods include:

- The duration of your employment;
- The length of time we have an ongoing relationship with you or your dependents/beneficiaries and the length of time thereafter during which we may have a legitimate need to reference your Personal Information to address issues that may arise;
- Whether there is a legal obligation to which we are subject (for example, certain laws may require us to keep your employment records for a certain period of time); and
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

GO TO TOP OF PRIVACY POLICY

6. What rights do you have regarding your Personal Information?

You may, subject to applicable law, make the following requests:

1. You may request that we disclose to you the following information:
    a. The categories of Personal Information we collected about you and the categories of sources from which we collected such Personal Information;
    b. The specific pieces of your Personal Information;
    c. The business or commercial purpose for collecting Personal Information about you; and
    d. The categories of Personal Information about you that we disclosed, and the categories of third parties to whom we disclosed such Personal Information.
2. You may request to correct inaccuracies in your Personal Information.
3. You may request that we delete your Personal Information that we have collected from you.

You have the right not to be unlawfully retaliated against for making a request under the CCPA. To make a privacy request, please contact us at https://compliance.snapon.com/RequestForm.aspx?co=SnapOnCorpHR&dl=en&rt=2 or 844-972-1285. We will verify and respond to your request consistent with applicable law, taking into account the type and sensitivity of the Personal Information subject to the request. We may need to request your name and address, in order to verify your identity and protect against fraudulent requests. If you maintain a password-protected account with us, we may verify your identity through our existing authentication practices for your account and require you to re-authenticate yourself before disclosing or deleting your Personal Information. If you make a request to delete, we may ask you to confirm your request before we delete your Personal Information.

Authorized Agents

If an agent would like to make a request on your behalf as permitted by applicable law, the agent may use the submission methods noted in the section entitled "What rights do you have regarding your Personal Information?" As part of our verification process, we may request that the agent provide, as applicable, proof concerning their status as an authorized agent. In addition, we may require that you verify your identity as described in the section entitled "What rights do you have regarding your Personal Information?" or confirm that you provided the agent permission to submit the request.

7. What are the sources of the Personal Information we have gathered?

We collect Personal Information from a variety of sources, including:

- Directly from you or your agent. For example, from documents or forms that you may provide to us to participate in Snap-on's health or retirement benefit programs or to apply for a job position. If you are providing personal information about another person, for example to name a beneficiary, please make sure you have their authority and inform them that we will use their information consistent with the purpose that you provided it to us.
- Indirectly from you or your agent. For example, from evaluating your performance in your job position or from references provided for your application for employment
- Directly and indirectly from your electronic activity on our websites, on our networks, or during your use of an online application or business system provided by Snap-on. For example, browsing history when you visit a website while on Snap-on's network, your downloads of programs to Snap-on equipment, or your use of Snap-on's email.
- From other members of the Snap-on Group.
- From Service Providers that provide services to us in connection with our business operations. For example, employee or candidate drug testing program administrators or employment applicant contact information from our applicant tracking system provider.
- From GPS tracking that may be in use on a company vehicle for fleet monitoring or on company applications, such as the list of calls and survey applications for Snap-on Tools employees.
- From Government agencies for purposes of verifying your eligibility for employment.

8. Who should I contact with questions about this Privacy Notice?

If you have any questions or comments about this Privacy Notice or need accommodation to access this Privacy Notice, you may contact your HR representative.

9. Modifications to this Privacy Statement

We reserve the right to modify this Privacy Notice at any time and without prior notice, subject to applicable legal requirements to notify you or obtain your consent. This version is dated July 1, 2023.