CALIFORNIA RESIDENTS

CALIFORNIA NOTICE AT COLLECTION (CCPA AND CPRA)

The California Privacy Rights Act ("CPRA") is an amendment to the California Consumer Privacy Act of 2018 ("CCPA"), effective January 1, 2023.Onto Innovation Inc. ("Company" or "we" or "our") is providing California residents this notice at collection ("Notice") to advise them of their rights granted by the CCPA and CPRA.

Purpose and Scope of the Notice

This Notice provides necessary information about the personal and sensitive information that the Company collects about California consumers, how it uses and shares this information. This Notice applies to all natural persons residing in California other than for a temporary or transitory purpose such as any employee, dependent, job applicant, independent contractor, investors and/or board member, ("Consumer" or "you" or "your").The Company will not sell the Personal Information that it collects. However, it may share this information with third party providers to meet its business needs. The Company will not sell the Sensitive Personal Information it collects, nor share it with third party providers for cross-context behavioral advertising.

Consumer Rights

As a California resident, you have the following rights under the CCPA:

1. **The right to know** what Personal Information we have collected about you, including the categories of Personal Information; the categories of sources from which the Personal Information is collected; the business or commercial purpose for collecting, selling, or sharing Personal Information; the categories of third parties to whom we disclose Personal Information; and the specific pieces of Personal Information we have collected about you. You may only exercise your right to know twice within a 12-month period.

2. **The right to delete Personal Information** unless a statutory exemption applies. Upon receiving a valid deletion request, we will delete your Personal information from our records within 45 calendar or 90 days if the deadline to delete has been extended with prior notice to you. If applicable, we will instruct any third-party providers to delete your information as well.

3. **The right to correct inaccurate Personal Information** maintained by the Company.

4. **The right to opt-out** of the sale or sharing of your Personal Information. We do not sell or share your Personal Information for cross-context behavioral advertising in any of the categories of Personal Information that we collect about California residents.

5. **The right to limit** the use and disclosure of Sensitive Personal Information collected about you. (for example, your social security number, financial account information, your precise geolocation data, or your genetic data) for limited purposes, such as providing you with the services you requested.

6. **The right not to receive discriminatory treatment** by the Company for the exercise of privacy rights conferred by the CCPA, in violation of California Civil Code § 1798.125, including an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights.

Children's Data

The Company may collect children's data for the provision of benefits, as well as enrollment in Company events. We do not sell Personal Information of Children under 16 years of age. Children between the ages of 13 and 16 can provide their own consent, but for children under the age of 13, the Company will obtain verifiable parental consent before collecting their Personal Information.

Method of Collection

The Company collects Personal Information from Consumers in person, over the phone, electronically using a website form, app, or product. The Company also uses cookies or online tracking technology for Consumers that access our website, ontoinnovation.com. This includes investors that sign up for investor alerts.

Storage and Retention

Personal Information as well as Sensitive Information may reside in Company servers, hard copies and in access controlled locked file cabinets. Your information shall be retained pursuant to Company policies for (i) as long as necessary for us to accomplish the business purpose; (ii) any duration necessary for complying with the laws and regulations; or (iii) for as long as necessary for the exercise or defense of legal rights and (iv) archiving, back-up, and deletion processes.

Disclosure of Personal Information

The Company may disclose Personal Information to:

1. Company affiliates-the information is made available only to those personnel who need access for authorized purposes such as relevant business managers, in-house counsel and authorized staff members.
2. Third parties and service providers- that provide products or services to us. For example, companies that support our website and help us with advertising or marketing, video conferencing , administrative or other services. The Company strives to enter into proper confidentiality and service agreements with these vendors. Examples of such parties include external auditors, outside counsel, insurance companies, travel service providers, IT service providers, payroll administrators, and employee benefit providers.
3. Law Enforcement personnel as required.

Business Purpose of Personal Information Collected

The Company collects Personal Information and Sensitive Personal Information to support its various business operations as listed in the table below. The table also lists, for each category, use purposes and whether the Company sells the information or shares it with third party providers for cross-context behavioral advertising.

Note: No Consumer data is sold or shared with any third-party providers in exchange for monetary or other valuable consideration.

Personal Information: The CCPA defines personal information as any information that either directly or indirectly:

1. identifies, relates to, or describes a particular consumer or household.
2. is reasonably capable of being associated with or could reasonably be linked to a particular consumer or household.

Personal Information does not include:

1. publicly available information
2. Lawfully obtained truthful information that is a matter of public concern.

3. Deidentified or aggregate consumer information

Personal Information Categories	Business Purpose	Shared with whom?
Identifiers: such as your full name, postal address, contact information, alias, gender, date of birth, signature, social security number, passport number, driver's license or state identification numbers, and similar information for your dependents and beneficiaries.	・Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks. ・Conduct employee onboarding. ・Maintain and administer payroll and employee benefit plans, including enrollment and claims handling. ・Maintain personnel records and comply with record retention requirements. ・Provide employees with human resources management services and employee data maintenance and support services. ・Communicate with employees and their emergency contacts and plan beneficiaries. ・Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. ・Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data management. ・Ensure employee productivity and adherence to Company policies. ・Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policies. ・Respond to law enforcement requests and as required by applicable law or court order. ・Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.	・Company affiliates, human resources personnel, relevant business managers, executives, in house counsel, information technology members, finance, payroll, and investor relations personnel who have a need to access for authorized purposes. ・Third parties and service providers that provide products or services to us. For example, vendors that support our website and help us with advertising or marketing, external auditors, outside counsel, insurance companies, travel service providers, IT service providers, payroll administrators, and employee benefit providers. ・Law enforcement agencies locally and overseas to support a claim or defense.

Protected classification characteristics under California or federal law: such as 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, pregnancy or childbirth and related medical conditions), military and veteran status.	· Comply with federal and state equal employment opportunity laws. · Administer employee benefits such as retirement, health, or other benefits, products, services to which employee or their dependents receive access through us. · Design, implement, and promote the Company's diversity and inclusion programs. · Perform workforce analytics, data analytics, and benchmarking. · Conduct internal audits, grievances, and suspected violations of Company policy. · Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.	· Company affiliates, human resources personnel, relevant business managers, executives, in house counsel, who have a need to access for authorized purposes. · Third parties and service providers that provide products or services to us such as internal research, reasonable accommodation, and employee benefits.
Commercial information: such as transaction information, purchase history, and financial details	· Provide reimbursement for business expenses, fixing accounting errors, maintaining accounts. · Respond to law enforcement requests and as required by applicable law or court order.	· Company affiliates, human resources personnel, relevant business managers, executives, finance, payroll. · Third-party providers who need access for processing transactions. · Law Enforcement personnel for fraud prevention.
Biometric information: such as facial recognition, and certain wellness metrics.	· Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents. · Administer and design health and wellness programs. · For marketing and communication, including photographs from events in which you voluntarily participated in whether for internal campaigns and/or external marketing.	· Law Enforcement locally and overseas including in-house counsel and outside counsel, executives, and relevant managers to support a claim or defense or for fraud prevention purposes. · Third party Providers who collect health and fitness data. · Marketing and advertising team.
Internet or other similar network, browsing, or search activity: including all activity on the Company's information systems (such as internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and	· Facilitate the efficient and secure use of Company information systems. · Ensure compliance with Company information systems, policies, and procedures. · Comply with applicable state and federal laws. · Prevent unauthorized access to, use, or disclosure or removal of the Company's property, records, data, and information.	· Company affiliates who need access for authorized purposes and/or required by the laws, locally and overseas, such as relevant business managers, human resources, authorized members of internal control functions, in house counsel and individuals from security and information technology.

passwords) and all activity on communications systems (such as phone calls, call logs, voicemails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of company-issued devices).	・Enhance employee productivity. ・Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policies. ・Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.	・Third party vendors providing auditing and ethics management services as well as outside counsel for handling claims. ・Law Enforcement agencies for fraud detection.
Geolocation data: such as the time and physical location related to use of an internet website, application, or device, and GPS location, and data from Company provided mobile devices of employees.	・Manage and monitor employee access to Company facilities, equipment, and systems. ・Investigate and enforce compliance with and potential breaches of Company policies and procedures. ・Exercise or defend the legitimate business interests and legal rights of Company and its employees	・Company affiliates who need access for authorized purposes and/or required by the laws, locally and overseas, such as relevant business managers, human resources, executives, in-house counsel and individuals from security and information technology. ・Law Enforcement agencies. ・Third parties such as outside counsel for claim handling.
Sensory and surveillance data: such as video, electronic, or audio surveillance and monitoring for security purposes. This would include call recordings and monitoring security badge use or IT login access	・Manage and monitor employee access to Company facilities, equipment, and systems. ・Investigate and enforce compliance with and potential breaches of Company policies and procedures. ・Administer and maintain Company operations, including for safety purposes. ・Exercise or defend the legitimate business interests and legal rights of the Company and its employees.	・Company affiliates who need access for authorized purposes and/or required by the laws, locally and overseas, such as relevant business managers, human resources, executives, inhouse and outside counsel and individuals from security and information technology. ・Third Party Providers providing services such as video conferencing. ・Law Enforcement agencies.
Professional or employment-related information: such as employment application information, work history, academic and professional qualifications, educational records, references, and interview notes, background check, drug testing results, work authorization, performance and disciplinary records, salary, bonus, commission, and other similar compensation data, benefit plan enrollment, participation, and claims information, leave of	・Recruit and process employment applications, including verifying eligibility for employment, background checks, and onboarding. ・Design and administer employee benefit plans and programs, including processing leaves of absence. ・Maintain personnel records and comply with record retention requirements. ・Communicate with employees and their emergency contacts and plan beneficiaries. ・Comply with applicable state and federal labor, employment, tax, benefits, workers' compensation,	・Company affiliates who need access for authorized purposes and/or required by the laws, locally and overseas, such as relevant business managers, human resources, in house counsel, authorized members of internal control functions, and individuals from security and information technology. ・Third Party Providers providing services such as employee management, recruitment, benefit provision, surveys, video services, and onboarding.

absence information including religious, military and family obligations, health data concerning employee and their family members.	disability, equal employment opportunity, workplace safety, and related laws. ・Prevent unauthorized access to or use of the Company's property, including its information systems, electronic devices, network, and data. ・Ensure employee productivity and adherence to the Company policies. ・Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policy. ・Evaluate and provide useful feedback about job performance, facilitate better working relationships, and for employee professional development. ・Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.	・Law Enforcement agencies.
Non-public educational information: such as education records, degrees and vocational certifications, report cards, and transcripts.	・Evaluate an individual's appropriateness for hire, or promotion or transfer to a new position at the Company.	・Company affiliates. who need access for authorized purposes and / or required by laws locally and overseas, such as human resources personnel, and relevant business managers. ・Third parties and service providers that provide products or services such as website support, recruiting services and engaging candidates for employment.
Inferences drawn from other personal information to create Consumer profiles: for example, an individual's preferences, abilities, aptitudes, and characteristics.	・N/A	・N/A

Sensitive personal information is a subtype of personal information consisting of specific information categories. While we collect information that falls within the sensitive personal information categories listed in the table below, the CCPA does not treat this information as sensitive because we do not collect or use it to infer characteristics about a person.

Sensitive Personal Information Category	**Business Purpose**	**Shared with whom?**

Government identifiers: such as your social security number, driver's license, state identification card, immigration status, or passport number.	▪ Recruit and process employment applications, including verifying eligibility for employment and conducting background and related checks. ▪ Process and administer payroll and employee benefit plans, including enrollment and claims handling. ▪ Maintain personnel records and comply with record retention requirements. ▪ Provide employees with human resources management services and employee data maintenance and support services. • Communicate with employees and their emergency contacts and plan beneficiaries. ▪ Comply with applicable state and federal labor, employment, tax benefits, workers' compensation, disability, equal employment opportunity, workplace safety, and related laws. ▪ Prevent unauthorized access to or use of the Company property, including information systems, electronic devices, network, and data. ▪ Respond to law enforcement requests and as required by applicable law or court order.	▪ Company affiliates who need access for authorized purposes and /or required by laws locally and overseas, such as human resources personnel, relevant business managers, authorized members of internal control functions, in house counsel and individuals from information technology, security finance, and payroll. ▪ Third parties and service providers providing administrative or other services to the Company including: travel service providers, outside counsel payroll administrator, and employee benefit providers. ▪ Law Enforcement agencies.
Complete account access credentials: such as usernames, financial account numbers, or card numbers combined with required access/security code or password.	▪ N/A	▪ N/A
Precise Geolocation such as physical access to a Company office location, or the location of a delivery, sales, or other employee in the field.	▪ Improve safety of employees, customers, and the public regarding use of the Company property and equipment. ▪ Prevent unauthorized access, use, or loss of the Company property. ▪ Improve efficiency, logistics, and supply chain management. ▪ Ensure employee productivity and adherence to the Company's policies. ▪ Conduct internal audits and investigate complaints, grievances,	▪ Company affiliates who need access for authorized purposes and /or required by laws locally and overseas, such as human resources personnel, relevant business managers, authorized members of internal control functions, in-house counsel and individuals from information technology, security finance, and payroll. ▪ Third parties and service providers providing

	and suspected violations of the Company's policies. · Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.	administrative or other services to the Company including: outside counsel, travel service providers, payroll administrator, employee benefit providers. · Law Enforcement agencies.
Racial or ethnic origin:	· Comply with federal and state equal employment opportunity laws. · Design, implement, and promote the Company's diversity and inclusion programs. · Perform workforce analytics, data analytics, and benchmarking. · Conduct internal audits and investigate complaints, grievances, and suspected violations of Company policies.	· Company affiliates. who need access for authorized purposes and/or required by Company policies, such as relevant executives, business managers, human resources, and in-house counsel . · Third parties and service providers that provide administrative, legal and other services.
Religious or philosophical beliefs:	· Review and process religious reasonable accommodation requests. · Exercise or defend the legal rights of the Company. and its employees, affiliates, customers, contractors, and agents.	· Company affiliates. who need access for authorized purposes and/or required by Company policies, such as relevant executives, business managers, human resources, in-house counsel and outside counsel. · Law Enforcement agencies, executives.
Mail, email, or text messages contents	· Conduct internal audits and investigate complaints, grievances, and suspected violations of the Company policies. · Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and agents.	· Company affiliates. who need access for authorized purposes and/or required by Company policies, such as relevant executives, business managers, human resources, in-house counsel, and outside counsel, security, and information technology. · Law Enforcement agencies, executives.
Genetic data: **such as DNA, RNA, genes, and chromosome information**	· N/A	· N/A
Unique identifying biometric information: **in order to establish individual identity**	· N/A	· N/A
Health information:	· Investigate and process workers' compensation claims. · Process health insurance claims	· Company affiliates. who need access for authorized purposes and/or required by Company

including job restrictions and workplace illness and injury information	• Comply with all applicable laws, regulations, and legal process.	policies, such as relevant executives, business managers, human resources in-house counsel, outside counsel Security and information technology. • Third Parties providing employee benefits such as workers compensation. • Law Enforcement agencies.
Sex life or sexual orientation information	• N/A	• N/A

Exercising your CCPA Rights

To submit a request to exercise your rights to know, delete, or correct your Personal Information , please email privacy@ontoinnovation.com, contact the Company at (978) 253-6200 or fill out the Privacy Information Request Form.

Only you, or someone legally authorized to act on your behalf, may make a request related to your Personal Information. You may authorize another person to submit a CCPA request on your behalf. You may also authorize a business entity registered with the California Secretary of State to submit a request on your behalf.

Please note that if you use an authorized agent, we may require more information from either the authorized agent or from you to verify that you are the person directing the agent. For example, for requests to know or delete your personal information, we may require the authorized agent to provide proof that you gave that agent signed permission to submit the request. The Company may also require you to verify your identity directly with us or directly confirm with us that you gave the authorized agent permission to submit the request.

Changes to the Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this Notice, we will post the updated notice on our website and update the effective date of the Notice.

Contact Information

For any questions or comments about our privacy policies and/or practices, please contact the Company at:
Email privacy@ontoinnovation.com or Info@ontoinnovation.com
Postal Address: 16 Jonspin Road, Wilmington Massachusetts MA 01887

Last Updated : November 1, 2023.