

EMPLOYMENT PRIVACY NOTICE

UNITED STATES- CALIFORNIA

Last Updated: January 1, 2023

Controlling Law:

As a California resident, during your interactions with us as an Employee, the processing of your personal data or “Personal Information” as defined by the California Privacy Rights Act of 2020 (“CPRA”) will occur under the terms of this Notice, as modified or supplemented these additional provisions, which are intended to capture applicable privacy rules, including the CPRA, as may be updated or amended.

A. Collection, Use, and Disclosure of Personal Data:

Micron collects all of the information described in Section 3 of our [Privacy Notice](#) from and about California residents. You should refer to that section for more detail, but this information generally falls into the categories listed in the chart below, to the extent it is personally identifiable. The chart also indicates the sources of the data, Micron’s purposes of processing, categories of third parties to whom we recently disclosed the data leading up to the effective date of this Notice, and how long we retain the categories of personal data in Micron systems.

Micron does not receive any monetary compensation for data it shares with vendors or service providers. Micron shares or “sold” (as that term is defined under the CPRA) “identifiers” (like IP addresses), “internet or other electronic network activity information” (like information regarding an individual’s browsing interactions on a website), and “commercial information” (like the fact that a browser visited our webpage,) to third parties that assist us, such as marketing or analytics providers.

EMPLOYMENT PRIVACY NOTICE

Categories of personal data Micron collects	Sources	Purpose(s) of processing personal data	Categories of third parties to whom we disclose	Retention of personal data
<p>Personal identifiers:</p> <p>Personal contact details such as name, title, address, date and place of birth, employee ID, telephone number and email address</p> <p>Bank account details, payroll records, and tax status information to verify and process payments</p> <p>Driver’s license number, passport number, nationality/visa status, or related information</p> <p>Social Security number, national identification number, or other government-issued numbers</p>	<p>(a) Directly or indirectly from you</p> <p>(b) From third parties</p>	<p>(a) Business purposes</p> <p>(b) Administering payments and benefits</p> <p>(c) Security measures and complying with health and safety obligations</p> <p>(d) Compliance</p>	<p>(a) Payroll services and benefits providers</p> <p>(b) Auditing and accounting firms</p> <p>(c) Professional services consultants</p> <p>(d) Vendors that assist with employment processes</p> <p>(e) Data analytics services</p> <p>(f) Security vendors</p> <p>(g) IT vendors</p> <p>(h) Professional service providers, including external auditors</p>	<p>Permanent</p>
<p>Protected Classifications and Sensitive Personal Data:</p> <p>Marital status and dependent information, information about disability, your race, ethnicity, religion, veteran’s status, or sexual orientation, health information, such as medical conditions and health and sickness records, background check information</p>	<p>(a) Directly or indirectly from you</p> <p>(b) From third parties</p>	<p>(a) Business purposes</p> <p>(b) Administering payments and benefits</p> <p>(c) Security measures and complying with health and safety obligations</p> <p>(d) Compliance</p>	<p>(a) Payroll services and benefits providers</p> <p>(b) Auditing and accounting firms</p> <p>(c) Professional services consultants</p> <p>(d) Vendors that assist with employment processes</p> <p>(e) Data analytics services</p> <p>(f) Security vendors</p> <p>(g) IT vendors</p> <p>(h) Professional service providers, including external auditors</p>	<p>Permanent</p>
<p>Biometric information:</p> <p>fingerprints, retinal scans, facial scans</p>	<p>Directly from you</p>	<p>(a) Security measures and complying with health and safety obligations</p>	<p>(a) Security vendors</p> <p>(b) IT vendors</p>	<p>3 years</p>

EMPLOYMENT PRIVACY NOTICE

Categories of personal data Micron collects	Sources	Purpose(s) of processing personal data	Categories of third parties to whom we disclose	Retention of personal data
<p>Internet or other similar network activity: Information about your use of Micron computers and networks, email or other electronic communications</p> <p>Information collected through cookies and similar technologies when browsing our website</p>	(a) Directly or indirectly from you	(a) Business purposes (b) Compliance	(a) IT vendors (b) Security vendors (c) Professional service providers, including external auditors	2 years
<p>Geolocation data</p>	(a) Directly or indirectly from you	(a) Security measures	(a) IT vendors (b) Security vendors (c) Professional service providers	5 years
<p>Sensory data:</p> <p>Audio, electronic, visual, thermal, olfactory, or similar information. Photographs, video conferencing recordings, CCTV recordings, telephone calls, communications over electronic channels and applications</p> <p>We do not routinely collect any of your thermal, olfactory or similar biometric information, but reserve the right to do so for site security or if health and safety concerns require us to do so.</p>	(a) Directly or indirectly from you	(a) Business purposes (b) Compliance	(a) IT vendors (b) Security vendors (c) Professional service providers	2-5 years
<p>Professional or employment-related information:</p> <p>Wages, salary, compensation, annual leave, retirement, work performance, disciplinary actions, grievances, and/or internal investigations, job titles, salary history, work history, working hours, holidays, absences, training records, professional memberships, board memberships, and other professional activities or roles.</p>	(a) Directly from you (b) From third parties	(a) Decisions related to employment (b) Business purposes (c) Compliance	(a) Vendors that assist with employment processes	Permanent

EMPLOYMENT PRIVACY NOTICE

Categories of personal data Micron collects	Sources	Purpose(s) of processing personal data	Categories of third parties to whom we disclose	Retention of personal data
Information from publicly available social media or networking sites or applications, and from other electronic search services.				
Education records: Grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	(a) Directly from you	(a) Decisions related to employment (b) Business purposes (c) Compliance	(a) Vendors that assist with employment processes	Permanent
Inferences drawn from other personal data collected: Information about additional skills that our systems infer that you may have.	(a) Directly from you (b) From third parties	(a) Decisions related to employment (b) Business purposes	(a) Vendors that assist with employment processes	3 years
Sensitive personal data or CPRA “sensitive personal information” collected: Social security number, driver’s license, state identification card, or passport number An 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. Precise geolocation Racial or ethnic origin, religious or philosophical beliefs, or union membership The contents of mail, email, and text messages unless the business is the intended recipient of the communication	(a) Directly from you (b) From third parties	(a) Business purposes (b) Administering payments and benefits (c) Security measures and complying with health and safety obligations (d) Compliance	(a) Payroll services and benefits providers (b) Auditing and accounting firms (c) Professional services consultants (d) Vendors that assist with employment processes (e) Data analytics services (f) Security vendors (g) IT vendors (h) Professional service providers, including external auditors	Permanent

EMPLOYMENT PRIVACY NOTICE

Categories of personal data Micron collects	Sources	Purpose(s) of processing personal data	Categories of third parties to whom we disclose	Retention of personal data
The processing of biometric information for the purpose of uniquely identifying an individual Personal information collected and analyzed concerning health Personal information collected and analyzed concerning sexual orientation				

B. Right to Opt Out of “Sale” of Personal data:

Californians have a right to ask us not to “sell or share” certain personal data as those terms are defined under the CPRA. You can make such a request by performing the following steps:

1. **Marketing opt-out:** Use the [“Your Privacy Choices”](#) link in the footer of Micron websites, click on the “opt-out” option to opt out of sharing and sales of your personal data, which includes any sharing of your information for targeted advertising. As an alternative to using the link referenced above, you may call +1-800-336-8915 between the hours of 8:00AM and 4:00PM Pacific Time to submit your request; and
2. **Cookies and online tracker opt-out:** If you’d like to opt-out of CPRA “sales or sharing” that happen through cookies and related technologies, follow the steps below on each Micron website you use:
 - a. Click the cookie icon in the bottom left corner of the website.
 - b. Select the “Reject All” option.

Please note, you must repeat this process for each device and browser that you use to access Micron websites.

C. Right to Limit Processing of Sensitive Personal data:

Micron processes sensitive personal data in its role as a prospective employer, but only for lawful purposes.

D. Right to Access, Correct, or Delete Personal data:

If you are a California resident, California law requires Micron to:

EMPLOYMENT PRIVACY NOTICE

- Provide you the categories of personal data we have recently collected or disclosed about you; the categories of sources of such information; the business or commercial purpose for collecting or disclosing your Personal data; the categories of third parties with whom we disclosed Personal data; and the length of time we retain this information.
- Upon request, provide a copy of personal data we hold about you, correct your personal data, or delete your personal data.

Please note, pursuant to the law, certain personal data is exempt from the above requests.

To exercise any of these rights, please use our [online form](#), or call +1-800-336-8915. Please note, we may request additional information from you, if necessary, to verify your identity or find your unique records in our systems.

We respect your right to privacy, and will not take any negative actions against you for asserting your rights.

E. Requests Made by Authorized Representatives:

If you are the authorized representative making an access, correction or deletion request on behalf of a California resident, we must take steps to verify your authority. This will require you to provide written proof of your authority.

F. Contacting Us:

You may contact us:

Via email: privacy@micron.com.

Via direct mail:

Micron Technology, Inc.
Attention: Legal - Privacy
8000 South Federal Way
Boise, Idaho 83707-0006, USA

Via telephone:1-800-336-8915