CALIFORNIA EMPLOYEE PRIVACY NOTICE

1. Purpose

This California Employee Privacy Notice (the "**Notice**") describes how MaxLinear, Inc. and our affiliates and subsidiaries (collectively, "**MaxLinear**," "**we**" or "**us**") collect and use personal information relating to our current and former employees and staff, as well as MaxLinear officers, directors and owners who are California residents (each an "**Employee**") and is intended to satisfy our notice and privacy policy requirements under the California Consumer Privacy Act and the regulations issued thereto, each as amended (collectively, the "**CCPA**").

The information in this Notice is intended to provide an overall description of our processing of Employee personal information. We may provide Employees additional notices about our data practices, such as those covered by other laws (e.g., if we conduct a background check). We encourage you to carefully read this Notice, together with any other privacy notice we may provide to you.

The personal information that we collect, and our use and disclosure of such personal information, may vary depending on the circumstances, such as your role and responsibilities with MaxLinear.

2. Scope

This Notice applies, generally, to the Employee personal information that we collect and otherwise process in the context of your employment relationship with MaxLinear, including personal information that we process to manage your working relationship, administer benefits, grant and control access to our systems and assets, and process Employee onboarding and terminations, as well as personal information we receive related to Employee beneficiaries, dependents and emergency contacts.

This Notice does not address or apply to our collection of personal information that is not subject to the CCPA, such as consumer credit reports and background checks, publicly available data, or other information that is exempt under the CCPA. This Notice also does not apply to the personal information we collect from contractors or job applicants, which is subject to different privacy notices, or to the personal information we collect about customers subject to the MaxLinear Privacy Policy.

3. Categories of Personal Information Collected Under California Privacy Law

The table below generally identifies the categories of personal information about Employees that we collect and have collected in the prior twelve (12) months, as well as the categories of third parties to whom we may disclose this information for a business or commercial purpose. In some cases (such as where required by law), we may ask for consent or give you certain choices prior to collecting or using certain personal information.

Categories of Personal Information	Third Party Disclosures for Business or Commercial Purposes
Identifiers: such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social	• service providers • advisors and agents • benefits providers

security number, driver's license number or other government identifiers.	• affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms • others as required by law
Paper and electronic records: records containing personal information, such as name, signature, photo, contact information, education and employment history, Social Security number and other government identifiers, insurance policy number, financial or payment information, medical information, or health insurance information.	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms • others as required by law
Characteristics of protected classifications Under California or Federal Law: such as race, sex, gender identity, age, national origin, disability, citizenship status, military/veteran status, marital status, medical condition, or other characteristics of protected classifications under California or federal law. (Note: generally, this information is collected on a voluntary basis and is used in support of our equal opportunity and diversity and inclusion efforts and reporting obligations, or where otherwise required by law).	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • others as required by law
Internet and Network Information: such as browsing history, search history, and information regarding interactions with an internet website, application, or advertisement, as well as physical and network access logs and other network activity information related to your use of any MaxLinear device, network or other information resource.	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms • others as required by law

Location Data: location information about a particular individual or device.	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms • others as required by law
Sensory Data: audio, electronic, visual, or similar information, such as, CCTV footage, photographs, and call recordings and other audio recordings (e.g., recorded meetings and webinars) or thermal temperature readings (which are not generally maintained on an individual employee basis).	• service providers • advisors and agents • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms • others as required by law
Professional or Employment-Related Information: such as information related to your employment history during the recruitment process.	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms • others as required by law
Education information: such as information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).	• service providers • advisors and agents • affiliates and subsidiaries • regulators, government entities and law enforcement • internet service providers, operating systems and platforms

	• others as required by law
Sensitive Personal Information: we may collect limited 'sensitive personal information' (as defined by the CCPA) from Employees, including: (a) Social Security number and other government identifiers (e.g., as part of the application and verification process); (b) racial or ethnic origin or sexual orientation (e.g., on a voluntary basis to support our equal opportunity and diversity and inclusion efforts and reporting obligations, or where otherwise required by law); (c) health information (e.g., as necessary to provide reasonable accommodations); and (d) precise geolocation (e.g., in connection with your timecard "punch" when you are a timecard employee).	• service providers • advisors and agents • benefits providers • affiliates and subsidiaries • regulators, government entities and law enforcement • others as required by law

We do not sell or share (as defined by the CCPA) personal information or sensitive personal information related to Employees, including those we know who are under the age of 16.

Sources of Personal Information. In general, we may collect the categories of personal information identified in the table above from the following categories of sources:

- Directly from the individual
- Our service providers, representatives, and agents
- Affiliates and subsidiaries

Retention. MaxLinear retains the personal information we collect only as reasonably necessary for the purposes described below or otherwise disclosed to you at the time of collection. For example, we will retain your information as necessary to comply with our tax, accounting, and recordkeeping obligations, to consider you for additional positions (with your permission), as well as an additional period of time as necessary to protect, defend or establish our rights, defend against potential claims, and comply with our legal obligations.

4. Purposes For Collecting Personal Information

Generally, we collect (and use and disclose) the above categories of personal information for the following purposes:

Compensation and benefits: relating to our administration of compensation and benefits, including:

- administering employee payroll, salary and compensation;
- administering employee pensions, IRAs and 401K, health insurance, medical plans, and other employee benefits administration (which may include the collection of personal information about others such as beneficiaries, where necessary to administer such benefits);
- reviewing, assessing and administering employee salary and compensation increases and bonuses;

- calculating deductions, issuing tax return-related documents and forms to employees;
- reviewing timecards and reported time worked; and
- monitoring and managing PTO, holiday, FMLA, and other leaves of absences.

Management of employment relationship: to manage our relationship with California Employees, including related to:

- hiring, terminations, relocation, transfers, promotions and disciplinary actions;
- providing employee accommodations;
- reviewing performance;
- conducting performance reviews, compensation and bonus reviews, and headcount and salary reviews;
- administering and monitoring compliance with our policies and procedures;
- maintaining records of emergency contact information for use in the event of an emergency;
- administering or performing employment contracts where applicable;
- conducting pre-employment and employment screening;
- for professional development and training purposes;
- verification and management of applicable credentials, licensing and other qualifications;
- facilitating employee communication and collaboration, such as through the corporate directory, employee bios and other similar; and
- in support of our equal opportunity employment policy and diversity and inclusion program.

Business operations and client services: relating to the organization and operation of our business and our performance of services to clients, including related to:

- operating our business by developing, producing, marketing, selling and providing goods and services;
- auditing and assessing performance of business operations, including client services and associated activities;
- performance, training and quality control;
- facilitating business development opportunities, as relevant; and
- facilitating communications in furtherance of the foregoing.

Security and monitoring: to monitor and secure our resources, network, premises and assets, including:

- monitoring for, preventing and investigating suspected or alleged misconduct or violations of work rules;
- monitoring for, preventing, investigating, and responding to security and privacy incidents;
- providing and managing access to physical and technical access controls;
- monitoring activities, access and use to ensure the security and functioning of our systems and assets; and
- securing our offices, premises and physical assets, including through the use of electronic access systems and video monitoring.

Health and safety: for health and safety purposes, such as contact tracing or conducting appropriate screenings of individuals prior to entering or accessing certain locations or premises.

Auditing, accounting and corporate governance: relating to financial, tax and accounting audits, and audits and assessments of our business operations, security controls, financial controls, or compliance with legal obligations, and for other internal business purposes such as administration of our records retention program.
M&A and other business transactions: for planning, due diligence and implementation of commercial transactions, for example mergers, acquisitions, asset sales or transfers, bankruptcy or reorganization or other similar business transactions.
Defending and protecting rights: to protect and defend our rights and interests and those of third parties, including to manage and respond to employee and other legal disputes, to respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, or the rights, interests, health or safety of others, including in the context of anticipated or actual litigation with third parties.
Complying with legal obligations: relating to compliance with applicable legal obligations (such as hiring eligibility, responding to subpoenas and court orders) as well as assessments, reviews and reporting relating to such legal obligations, including under employment and labor laws and regulations**,** Social security and tax laws**,** environmental regulations, workplace safety laws and regulations, and other applicable laws, regulations, opinions and guidance.

Sensitive Personal Information. Notwithstanding the purposes described above, we do not collect, use or disclose of sensitive personal information about Employees beyond the purposes authorized by the CCPA (pursuant to Cal Civ. Code § 1798.121 and § 7027 of the CCPA regulations). Accordingly, we only use and disclose sensitive personal information about Employees as reasonably necessary and proportionate: (i) to perform our services requested by you; (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents; (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct; (iv) to verify or maintain the quality and safety of our services; (v) for compliance with our legal obligations; (vi) to our service providers who perform services on our behalf; and (vii) for purposes other than inferring characteristics about you.

5. Your Rights Under California Law

Employees who are residents generally have the following rights under California Privacy Law with respect to their personal information processed by us, subject to certain limitations and exceptions.

- Deletion: the right to request deletion of their personal information that we have collected about them.
- Know/access: the right to know what personal information we have collected about them, 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 them.

- Correction: the right to request correction of inaccurate personal information we maintain about them.
- Opt out of sales and sharing: the right to opt-out of the sale and sharing of their personal information. However, as discussed above, we do not sell or share Employee personal information, thus this right is not available to Employees.
- Limit use/disclosure of sensitive personal information: the right to request to limit certain uses and disclosures of sensitive personal information. However, as discussed above, we do not use or disclose Employee sensitive personal information beyond the purpose authorized by the CCPA, thus this right is not available to Employees.
- Non-discrimination: the right not to be subject to discriminatory treatment for exercising their rights under the CCPA.

Submitting CCPA Requests. Employees may exercise their California privacy rights as set forth above by submitting a request through a California Privacy Request or calling 1-800-227-7103.

We will take steps to verify your request by matching the information provided by you with the information we have in our records. Your request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative (i.e., by completing all required fields on our webform if you choose to submit a request in that manner).

- Describe your request with sufficient details that allows us to properly understand, evaluate, and respond to it.

In some cases, we may request additional information in order to verify your request or where necessary to process your request.

Authorized agents may initiate a request on behalf of another individual by contacting us at webmaster@maxlinear.com. Authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.

6. Contacting Us About This Notice

If you have questions or concerns regarding this Notice or the handling of your personal information, please contact us at PrivacyCA@maxlinear.com .

EFFECTIVE DATE: *January 1, 2023*