

EU U.S. DATA PRIVACY FRAMEWORK POLICY

I. OVERVIEW.

Photronics Inc. (including its subsidiaries set forth on Schedule I attached hereto) (collectively, “Photronics” or “our”) is committed to respecting the privacy of its employees, customers, and business partners in a lawful, fair, and transparent way.

Photronics complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPFs set forth by the U.S. Department of Commerce. Photronics has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

II. DEFINITIONS.

“Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

“Data Subject” means all individuals whose Personal Data are Processed by Photronics, including current, future, and former employees, customers, suppliers, other contractual partners, and website visitors.

“Identifiable” means if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is “identifiable.”

“Personal Data” & “Personal Information” are data about an identified or identifiable individual that are within the scope of the GDPR, received by an organization in the United States from the EU, and recorded in any form.

“Processing” of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

“Sensitive Data” means information about a Data Subject’s race or ethnicity, religious or philosophical beliefs, sexual orientation, trade union membership, and political opinions; a Data Subject’s health, including any medical condition, health and sickness records, including where they leave employment and under any benefits plan operated by Photronics the reason for leaving is determined to be ill- health, injury, or disability, the records relating to that decision; details of any absences (other than holidays) from work including time on

statutory parental leave and sick leave; where you leave employment and the reason for leaving is related to a Data Subject's health, information about that condition needed for pensions and permanent health insurance purposes; genetic information and biometric data; and information about criminal convictions and offenses.

III. USE OF PERSONAL DATA AND SENSITIVE DATA.

Photonics will only use Personal and/or Sensitive Data when the law allows us to. Unless otherwise permitted by applicable law, Photonics will only use Personal and/or Sensitive Data if:

- The Data Subject has declared his/her consent;
- The Data Subject has manifestly made public such data;
- It is necessary to perform a contract Photonics has entered into with a Data Subject;
- It is necessary to comply with a legal obligation or establish a legal claim or defense;
- It is required in response to a lawful request by a public authority, including for purposes of national security or law enforcement requirements or otherwise required pursuant to applicable law; and
- It is necessary for our legitimate interests (or those of a third party) and a Data Subject's interests and fundamental rights do not override those interests.

Photonics may also use Personal and/or Sensitive Data in the following situations, which are likely to be rare:

- Where it is in the vital interests of the Data Subject (or someone else's interests).
- Where it is necessary in the public interest or for official purposes.

Photonics may Process Personal and/or Sensitive Data about a Data Subject for all purposes permissible under applicable laws, including, but not limited to:

- Human Resources and personnel management, such as staffing; recruiting; verifying background and qualifications (if and when relevant to job functions and in compliance with the law); offering and administering payroll, insurance, and other benefits including pensions and stock options including stock purchase programs; managing work-related expenses; evaluating performance; training and career development; managing disciplinary and termination processes; responding to personnel grievances; enforcing compliance with internal policies; providing relocation related, travel, or other mobility related support; complying with applicable legal requirements; and performing other administrative and managerial tasks.

Business operations, such as engaging a prospective party in business transactions including the purchase, sale, lease, merger, or other type of acquisition, disposal, securitization or financing (in whole or in part) involving Photonics; managing the company's assets; selecting, managing, and deploying contractors, vendors, suppliers, advisors, other professional experts, and Photonics personnel to perform work for Photonics; providing IT, finance, legal, and management services such as strategic planning, budgeting and financial forecasting, allocation of human resources, research and development, real estate and property management, storage, and computing;

safeguarding IT infrastructure, equipment, and other Photronics property and ensuring business continuity; preventing and managing security incidents and providing security services; administering occupational health and safety initiatives; authenticating worker status to authorize access to Photronics resources and facilities or to assist in authorizing access to Photronics client facilities; operating maintenance departments; maintaining business records, compiling audit trails, and implementing other reporting tools; contacting or assisting personnel and others in case of emergency; and other general administrative and operation tasks.

- Compliance with legal and other requirements, such as duties under labor laws and regulations; record-keeping and reporting obligations; government requests, inspections, and investigations; responding to legal process such as subpoenas; protecting the legal rights of Photronics, our personnel, or others; detecting and preventing crime, fraud, and conflicts of interests; auditing compliance with Photronics standards, procedures, and contractual obligations; and in the good faith belief that such use is necessary to adhere to applicable laws or perform any of the purposes herein.
- In some cases, Photronics may collect Personal Data (including Sensitive Data) about family members, close personal relationships, beneficiaries, and emergency contacts for certain purposes described below (such as the provision of health care or life insurance benefits to you or a Data Subject's dependents or in case you experience a medical emergency at work). If a Data Subject provides Personal Data about others, Photronics will rely on a Data Subject (unless otherwise required by law) to communicate to those individuals that a Data Subject is providing us with their Personal Data, to inform them that they continue to have privacy rights in such Personal Data, and to obtain their consent, as necessary, for us to Process their Personal Data (including explicit consent where necessary for the collection and disclosure of Sensitive Data). Photronics will respect the privacy rights of those individuals.

IV. NOTICE.

- Photronics notifies Data Subjects about: the types of personal data collected, and where applicable, the entities or subsidiaries of Photronics also adhering to the Principles; Photronics' commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF; the purposes for which Photronics collects and uses Personal Data; how to contact Photronics with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints; the type or identity of third parties to which Photronics discloses personal information, and the purposes for which it does so; the right of individuals to access their personal data; the choices and means Photronics offers individuals for limiting the use and disclosure of their personal data; the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to Data Subjects whether it is (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States; being subject to the investigatory and enforcement powers of the FTC other U.S. authorized statutory body, the possibility, under certain conditions, for Data Subjects to invoke binding arbitration; the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; and Photronics' liability in cases of onward transfers to third parties.

V. CHOICE.

If Personal Data covered by this EU-U.S. DPF Policy is to be used for a new purpose that is materially different from that for which the Personal Data was originally collected or subsequently authorized, or is to be disclosed to a third party, Photronics will provide Data Subjects with an opportunity to choose whether to have their Personal Data so used or disclosed. Requests to opt out of such uses or disclosures of Personal Data should be sent to: privacy@photronics.com.

If Sensitive Data covered by this EU-U.S. DPF Policy is to be used for a new purpose that is different from that for which the Personal Data was originally collected or subsequently authorized, or is to be disclosed to a third party, Photronics will obtain the Data Subject's explicit consent prior to such use or disclosure. Photronics will not subject Data Subjects to decisions that will have a significant impact on them based solely on automated decision-making, unless Photronics has a lawful basis for doing so and has notified a Data Subject.

Photronics may share Personal Data with its affiliates and subsidiaries. Photronics may disclose Personal Data without offering an opportunity to opt out in response to valid requests by public authorities, including to meet national security or law enforcement requirements. Photronics also reserves the right to transfer Personal Data without consent under any circumstances permissible under respective applicable national laws and regulations.

VI. ACCOUNTABILITY FOR ONWARD TRANSFER OF PERSONAL DATA.

Photronics may transfer Personal Data to its third-party agents or service providers who perform functions or acts as a controller on its behalf with compliance to the aforementioned Notice and Choice provisions of the Principles. Where required by the EU-U.S. DPF, Photronics has or will enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection the EU-U.S. DPF requires and limiting their use of the data to the specified services provided on its behalf. Photronics takes reasonable and appropriate steps to ensure that third-party agents and service providers Process Personal Data in accordance with Photronics' EU-U.S. DPF obligations and to stop and remediate any unauthorized Processing. Under certain circumstances, Photronics may remain liable for the acts of our third-party agents or service providers who perform services on our behalf for their handling of Personal Data that Photronics transfer to them. A Data Subject may also request that Photronics transfer Personal Data to another party.

To transfer personal data to a third party acting as an agent, Photronics will: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with Photronics' obligations under the Principles; (iv) require the agent to notify Photronics' if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of Photronics' its contract with that agent to the Department

upon request

VII. SECURITY.

Photronics maintains reasonable and appropriate security measures when creating, maintaining, using or disseminating Personal Data to protect it from loss, misuse, unauthorized access, disclosure, alteration, or destruction in accordance with the EU-U.S. DPF taking into due account the risks involved in the processing and the nature of the personal data.

VIII. DATA INTEGRITY AND PURPOSE LIMITATION.

Photronics limits the collection of Personal Data covered by this EU-U.S. DPF Policy to information that is relevant for the purposes of Processing. Photronics does not Process such Personal Data in a way that is incompatible with the purposes for which it has been collected or authorized by the Data Subject.

Photronics takes reasonable steps to ensure that Personal Data is reliable for its intended use, accurate, complete, and current. Photronics takes reasonable and appropriate measures to comply with the requirement under the EU-U.S. DPF to retain Personal Data in identifiable form only for as long as it serves a purpose of Processing. Photronics will only retain Personal Data for as long as necessary to fulfil the purposes Photronics collected it for, including for the purposes of satisfying any legal, accounting, auditing, security and fraud prevention, preserving or defending the organization's legal rights, reporting requirements or other purposes consistent with the expectations of a reasonable person given the context of the collection. This obligation does not prevent Photronics from processing Personal Data for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research and statistical analysis. To determine the appropriate retention period for personal data, Photronics considers the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of the Personal Data, the purposes for which Photronics may Process the Personal Data, whether Photronics can achieve those purposes through other means, and the applicable legal requirements. Photronics will adhere to the EU-U.S. DPF Principles for as long it retains Personal Data.

IX. ACCESS.

Data Subjects generally have the right to access the Personal Data held by Photronics and to request that Photronics correct, amend, or delete it if it is inaccurate or Processed in violation of the EU-U.S. DPF Principles. These access rights may not apply in some cases, including where providing access is unreasonably burdensome or expensive under the circumstances or where it would violate the rights of someone other than the individual requesting access. If you would like to request access to, correction, amendment, or deletion of Personal Data, you can submit a written request to the contact information provided below. Photronics may request specific information from you to confirm a Data Subject's identity.

X. RECOURSE, ENFORCEMENT AND LIABILITY.

The Federal Trade Commission has jurisdiction over Photronics' compliance with the

EU-U.S. DPF.

Data Subjects may file a complaint concerning Photronics' Processing of their Personal Data. The complaint should be sent to privacy@photronics.com. Photronics will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of Personal Data within 45 days of receiving a complaint. For any unresolved complaints, Photronics commits to cooperate with the EU data protection authorities. A Data Subject may submit its complaint to the appropriate resolution panel of the responsible data protection agency (DPA). Photronics will ensure that a Data Subject does not incur any costs in its application to the DPA. The decision of the DPA shall be binding upon Photronics. Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm. Photronics has further committed to refer unresolved privacy complaints under the EU-U.S. DPF Principles to an independent dispute resolution mechanism, the alternative dispute resolution provider JAMS (Judicial Arbitration and Mediation Services). If a Data Subject does not receive timely acknowledgment of its complaint, or if a Data Subject's complaint is not satisfactorily addressed, they may visit [Data Privacy Framework Resolution | JAMS Mediation, Arbitration, ADR Services \(jamsadr.com\)](#) for more information and to file a complaint.

If a EU-U.S. DPF complaint cannot be resolved through the above channels, under certain conditions, a Data Subject may invoke binding arbitration for claims not resolved by other redress mechanisms. In certain circumstances, the EU-U.S. DPF Framework provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the EU-U.S. DPF Principles.

Should Photronics become subject to an FTC or court order based on non-compliance with the Principles, Photronics will make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Photronics commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF in the context of the employment relationship.

XI. CHANGES TO THIS PRIVACY NOTICE PRIVACY NOTICE.

Photronics reserves the right to update this Privacy Policy at any time in accordance with the EU-U.S. DPF Principles. In the event material changes are made, a new Privacy Policy will be issued.

XI. HOW TO CONTACT PHOTRONICS.

For questions or concerns about this Policy or the other privacy policies, please send an email to privacy@photronics.com or contact our Corporate Legal Department at:

Photronics, Inc.
Attention: Corporate Legal Department
15 Secor Road
Brookfield, CT 06804
(203) 740-5601

SCHEDULE I

Photronics Idaho, Inc.
Photronics Texas Allen, Inc.