EMPLOYEE DATA PRIVACY POLICY

Amended and Restated April 23, 2012

Oclaro, Inc., including our affiliates and subsidiaries (collectively referred to as the "Company", "we", "us" or "our"), appreciates your service to the Company. The privacy and security of the personal data collected from you ("Organization Human Resources Data") is a Company priority. It is equally important to us that you understand how we handle this data. We adhere to the Safe Harbor Agreement concerning the transfer of Organization Human Resources Data from the European Union ("EU") and Switzerland to the United States of America ("U.S."). Accordingly, we follow the Safe Harbor Principles published by the U.S. Department of Commerce (the "Principles") with respect to such data. This privacy policy outlines our general policy and practices for implementing the Principles, including the types of information we gather, how we use it and the notice and choice affected individuals have with respect to our use of and their ability to correct such information.

Collection and Use of Data

To conduct business and comply with government regulations, we collect various personal and other data depending on your employment responsibilities, citizenship, location of employment and other factors. Such data may include your name, user ID's, phone numbers, e-mail address, mailing addresses, banking and other financial data, government identification numbers (such as, but not limited to, your social security number, taxpayer identification number and driver license information), date of birth, gender, race, ethnicity, health and disability data, family-related data (such as, but not limited to, your marital status and personal and health-related data regarding your family members) trade union data and any other necessary data. We use your information to conduct business and comply with government regulations. Such use includes, but is not limited to, the following uses: to identify you personally; to communicate with you; to provide employee benefits; to comply with human resource requirements; and to comply with government regulations.

Disclosure of Data

We will not disclose, sell or otherwise distribute to any third party any of your personally identifiable data without your prior permission (or you may opt out of such disclosure) except under the following circumstances:

> Legal requests and investigations. We may disclose any data about you when, in our opinion, such disclosure is necessary to prevent fraud or to comply with any statute, law, rule, or regulation of any governmental authority or any order of any court of competent jurisdiction. Further, we agree to cooperate in

investigations by and to comply with the advice of competent EU authorities in such cases.

Third-party service providers. We may, from time to time, outsource some or all of the operations of our business to third-party service providers. In such cases, it may be necessary for us to disclose your data to those service providers. In some cases, the service providers may collect data directly from you on our behalf. We restrict how such service providers may access, use and disclose your data.

Agents. We employ other companies and individuals to perform functions on our behalf. Examples include processing compensation, providing employee benefits and performing legal and other professional services. These agents have access to your data needed to perform their functions, but they may not use it for other purposes.

Business Transfers. As we continue to develop our business, we may sell our companies, subsidiaries or business units. In such transactions, data generally is one of the transferred business assets. Also, in the event that the Company or all of its assets are acquired, your data may be one of the transferred assets.

Protection of Company and Others. We release data when we believe it is appropriate to comply with the law; enforce or apply our policies and other agreements; or protect the rights, property or safety of the Company, our employees or others. However, this does not include selling, renting, sharing or otherwise disclosing personally identifiable data from employees for commercial purposes other than as set forth in this privacy policy.

Updating and Accessing Your Organization Human Resources Data

You must immediately update your data when and if it changes so that we can maintain accurate data about you. Although you may change your data, we may maintain such prior data about you. Therefore, you should not expect that all of your historical data will be removed from our databases at the time you notify us of changes. To access, change or remove your data, you may contact the Company's Human Resources department by phone or e-mail. The Company allows employees the opportunity to correct, amend or delete inaccurate information, except where the burden or expense of providing access would be disproportionate to the risks to privacy of the individual, or where the rights of persons other than the requesting employee would be violated. The Company shall process your data in a way that is compatible with and relevant for the purpose for which it was collected or authorized by you. To the extent necessary for those purposes, the Company will take reasonable steps to ensure that your data is accurate, complete, current and reliable for its intended use.

Security of Your Organization Human Resources Data

The Company has put in place reasonable security measures and technologies, physical, electronic and managerial procedures to safeguard and secure Organization

Human Resources Data from loss, misuse, unauthorized access or disclosure, alteration or destruction. If you are authorized to have access to the Organization Human Resources Data of others, it is important that you take the appropriate safeguards to protect this Organization Human Resources Data. Paper and other hard copies containing Organization Human Resources Data should be secured in a locked location when not in use. Computers and other access points should be secured when not in use by logging out or locking. Passwords should be guarded and not shared. When no longer necessary for business purposes, paper and hard copies should be immediately destroyed using paper shredders or other approved devices. Do not make or distribute unauthorized copies of documents or other tangible mediums containing Organization Human Resources Data. Electronic files containing Organization Human Resources Data should only be stored on secured computers and not copied or otherwise communicated to unauthorized individuals within or outside of the Company.

Compliance with this privacy policy is important to the Company. Any potential violation of these privacy policies should be reported to your manager. Failure to follow these privacy policies may result in discipline of the employee. Any questions or suggestions regarding these policies may also be directed to your manager.

U.S.-EU and U.S.-Swiss Safe Harbor

Organization Human Resources Data from the EU, Switzerland and/or citizens from any of the above referenced regions may be collected by us and may be stored and processed in the U.S. or any other country in which the Company or its affiliates, subsidiaries or agents maintains facilities. By your employment at the Company, you consent to any such transfer of data outside of your country. The Company abides by the privacy principles of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks and has certified its adherence to the Safe Harbor Privacy Principles with the U.S. Department of Commerce regarding the collection, use and retention of data from the EU and Switzerland. The Company uses a self-assessment approach to assure compliance with this privacy policy and periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, appropriately displayed, implemented and accessible and in conformity with the Principles. We encourage employees to raise any concerns that they may have concerning our privacy policy. If you believe your privacy may have been violated based on the principles set forth in the Safe Harbor framework, please contact the Human Resources department in writing providing a description of the possible violation. The Company will investigate and attempt to resolve any such possible violation. If you do not find the proposed solution satisfactory, the Company will engage the services of a third party to serve as its independent recourse mechanism (IRM) for Safe Harbor-related dispute resolution. If such a case arises, the Company will use the EU Data Protection Authorities and/or the Swiss Federal Data Protection and Information Commissioner to investigate such unresolved complaint(s).

Amendments
This privacy policy may be amended from time to time consistent with the requirements of the Safe Harbor and our business practices. We will post any revised policy on the Company's website.

Information Subject to Other Policies
The Company is committed to following the Principles for Organization Human Resources Data within the scope of the Safe Harbor Agreement. However, certain information is subject to policies of the Company that may differ in some respects from the general policies set forth in this privacy policy.

Contact Information
Questions, comments or complaints regarding the Company's Safe Harbor Policy or data collection and processing practices can be mailed or e-mailed to:

Oclaro, Inc.
Worldwide Headquarters
Attn: David Teichmann
2560 Junction Ave.
San Jose, CA 95134
david.teichmann@oclaro.com