

Bourns, Inc. EU Policy

I. Objective

Bourns, Inc. (“Bourns”) wishes to set forth in a formal corporate policy the principles under which Bourns processes Personal Data (defined in Section 3.3 below) received from countries belonging to the European Union (“EU”).

II. Background

The EU has adopted a Directive on Data Protection (“EU Directive”) that requires EU member states to adopt laws protecting Personal Data collected within their borders. These laws must, among other provisions, restrict the transfer of Personal Data only to countries that have data protection laws deemed “adequate” under standards established in the EU Directive. Bourns has subsidiaries located in the EU and intends to comply with the individual country laws meeting the EU Directive’s requirements with respect to Personal Data Bourns collects and processes through the employment relationship. The United States Department of Commerce has published a group of privacy principles set forth at www.export.gov/safeharbor which constitute core data protection principles acceptable to the EU Member States (the “Safe Harbor Principles”). The EU has determined that companies that comply with the Safe Harbor Principles satisfy the adequacy requirements of the EU Directive and that the Personal Data of EU residents may be transferred to these companies notwithstanding the fact that they may be located in countries with data protection laws that have not been deemed “adequate” by the proper authority in the EU. Bourns has developed and adopted this comprehensive Policy on Data Protection and Privacy of Personal Information (“Privacy Policy”) to adhere to the Safe Harbor Principles.

III. Definitions

3.1 Identifiable Person - means a natural person that is or can be identified, directly or indirectly, as a particular person by reference to an identification number or to one or more aspects of the person’s physical, physiological, mental, economic, cultural or social identity. Identifiable Persons may include any employee, applicant, former employee, or retiree of Bourns or its subsidiaries in the EU.

3.2 Personal Data - is any information about an Identifiable Person that

- (i) is within the scope of the EU Directive,*
- (ii) is received by Bourns in the U.S. from the EU,*
- (iii) is recorded in any form and*

(iv) identifies the Identifiable Person or could reasonably be used to identify the Identifiable Person regardless of the recording medium involved, e.g., paper, electronic or video.

3.3 Processing - means any online or offline processing and includes such activities as copying, filing, and inputting personal information into a database.

3.4 Sensitive Data - is data that pertains to medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation or any other data that is identified as “sensitive” by the Identifiable Person.

IV. Publication

This Privacy Policy will be published in Bourns Corporate Policy Manual (CPM) - Administration, Section 1.7 - Human Resources and on the web at <http://www.bourns.com/>.

V. Policy And Procedure

5.1 Notice

5.1.1 Bourns notifies all Identifiable Persons that it collects, processes and uses Personal Data as an employer or a potential employer only in a lawful manner and in compliance with the Safe Harbor Principles.

5.1.1.1 To the extent practical and appropriate, Bourns collects Personal Data directly from the Identifiable Person. In those cases where Bourns collects Personal Data from other persons, it takes measures to respect the privacy preferences of the Identifiable Persons. Examples of when Bourns may seek information from others include, without limitation, evaluating employees, recruiting, benefit administration and succession planning.

5.1.1.2 Bourns’ collection and use of Personal Data in the employment context is essential to the conduct of Bourns’ human resources and business functions. Examples of the purposes for which Bourns collects and uses Personal Data include, without limitation, recruitment, payroll, and personnel management, such as compensation, promotion, evaluation, benefit administration and succession planning.

5.1.1.3 While recognizing that all Personal Data deserves to be protected, Bourns exercises special precautions and

safeguards for Sensitive Data. Unless required by applicable law, Bourns does not request or record Sensitive Data.

5.1.1.4 This Privacy Policy does not apply to information that is “anonymized” so that the identities of Identifiable Persons are not known to Bourns.

5.2 Choice

5.2.1 Opt-Out Rights. Bourns may share Personal Data with its subsidiaries or use Personal Data for a purpose incompatible with the reason the Personal Data was originally collected. In such circumstances, Bourns will first provide each Identifiable Person with the opportunity to opt-out of such sharing of his or her Personal Data in accordance with the Safe Harbor Principles. In addition, where consent of Identifiable Persons or their representatives is required by law, contract, or agreement for the collection, use, or disclosure of Personal Data, Bourns will request such consent and respect the Identifiable Person’s choice in such matters.

5.2.1.1 Bourns is not required to provide notice in certain circumstances as specified or permitted by the Safe Harbor Principles or applicable law, such as when it would compromise the ability of Bourns to respond to legal process.

5.2.1.2 In certain limited or exceptional circumstances, in accordance with the Safe Harbor Principles, Bourns may disclose Personal Data without the consent of the Identifiable Person. For example, this may occur when Bourns is required to disclose information by law or legal process or in the vital interests of the Identifiable Person, such as when life or health are at stake.

5.2.2 Opt-In Requirement. Except as provided by the Safe Harbor Principles or applicable law, an Identifiable Person must give affirmative permission (opt in consent) before Bourns will disclose Sensitive Data to a third party or use Sensitive Data for a purpose other than those for which it was originally collected or subsequently authorized by the Identifiable Person.

5.3 Onward Transfer

5.3.1 Bourns may transfer Personal Data across state and country borders for the purposes of data analysis and consolidation of Human Resource information worldwide. Bourns will comply with the provisions of this Privacy Policy in any such transfer.

5.3.2 To enable Bourns to provide employees with certain

services such as payroll direct deposit, personnel benefits, or other human resource services, Bourns may disclose Personal Data without consent to sub-contractors, vendors or other third parties, if the third party (i) subscribes to the Safe Harbor Principles, (ii) is subject to laws meeting the minimum standards required by the EU Directive or (iii) enters into an agreement with Bourns obligating the third party to provide at least the same level of privacy protection as required by Safe Harbor Principles.

5.4 Security

5.4.1 Bourns takes reasonable precautions to protect Personal Data against loss, misuse and unauthorized access, disclosure, alteration, destruction and theft.

5.4.1.1 These precautions include password protections for online information systems and restricted access to Personal Data. All inquiries from outside Bourns, whether written or oral, concerning the identity, employment record or performance of an employee or former employee must be referred to the Human Resources Department.

5.4.1.2 Employees are responsible for helping maintain security through safeguarding Personal Data, e.g., by protecting passwords used to access Bourns computer systems, by keeping paper records under lock and key when not in use, and by disposing of files and reports no longer needed in a secure manner.

5.5 Data Integrity

5.5.1 Bourns takes reasonable steps to keep Personal Data accurate, complete, and up-to-date. Each Identifiable Person is responsible for informing Bourns or its EU subsidiaries of any changes in Personal Data so that the information that Bourns holds about him or her is accurate, complete and up-to-date.

5.5.2 Bourns retains Personal Data only as long as necessary to meet the purposes for which it was collected or as required by law, contractual agreement, or the Safe Harbor Principles.

5.5.2.1 Certain Personal Data may be archived to administer post-employment benefits, to meet legal requirements, to provide evidence in cases of litigation, for statistical purposes, or to assist in decision relating to re-employment.

5.5.2.2 Bourns uses reasonable procedures, following retention guidelines, to ensure that it archives or destroys Personal Data no longer required for the purposes for

which it was originally collected, unless otherwise agreed to by the Identifiable Person.

5.6 Access

5.6.1 Bourns provides Identifiable Persons with a reasonable opportunity to examine their Personal Data, to challenge its accuracy and to have it corrected, amended or deleted as appropriate, subject to certain exceptions.

5.6.2 Upon request, Identifiable Persons will be given reasonable access to the Personal Data Bourns holds about them. Reasonable access applies to both the process of accessing Personal Data and the types of Personal Data to be accessed.

5.6.2.1 Reasonable access means that requests for access are made during normal business hours, following standard procedures, and that the frequency of access requests is not excessive.

5.6.2.2 If an Identifiable Person is denied access, Bourns will provide such Identifiable Person with the reason(s) for denying access and a contact point for further inquiries.

5.6.3 If the Identifiable Person notifies Bourns that the Personal Data on file is incorrect and provides Bourns with appropriate supporting documentation, Bourns will either correct the Personal Data or direct the Identifiable Person to the source of the information for correction.

5.6.3.1 If, upon review, Bourns believes that the existing Personal Data is correct, Bourns will inform the Identifiable Person. If the Identifiable Person continues to dispute the accuracy of the Personal Data, Bourns will note that dispute in the record of the Identifiable Person upon written request.

5.6.4 The Safe Harbor Principles provides for some exceptions to the obligation to provide access to Personal Data. Access to confidential or proprietary information, such as business reorganization or succession plans, or where granting access has to be balanced against the privacy interests of others, may be restricted. In addition, access may be denied

- (i) *when the information requested relates to an ongoing investigation, litigation or potential litigation,*
- (ii) *where the burden or expense of providing access would be disproportionate to the risks to the privacy of the Identifiable Person or*
- (iii) *when the rights of persons other than the Identifiable Person would be violated.*

5.7 Enforcement

5.7.1 Identifiable Persons may contact the Vice President - Corporate Administration at Corporate Headquarters in Riverside, California to submit data access requests, register complaints or address any other relevant issues under the Safe Harbor Principles.

5.7.1.1 If a complaint about the processing and/or transfer of Personal Data is not resolved to the satisfaction of the Identifiable Person through internal procedures, then Bourns will refer such person to the Data Protection Authority in the jurisdiction where the person works or the United States Federal Trade Commission, at the option of Bourns. Bourns will cooperate with such authorities in the investigation of any unresolved complaints.

5.7.1.2 Bourns is committed to assisting Identifiable Persons in protecting their privacy and in exercising their rights under this Privacy Policy and applicable laws. Identifiable Persons making complaints or reporting potential violations of the Privacy Policy shall not be subject to any form of retaliation. In addition, report of potential violations may be made on an anonymous basis.

5.7.2 It is the responsibility of all employees to act in accordance with the Privacy Policy and obligations with respect to Personal Data. Failure to do so may result in disciplinary action, if warranted, up to and including termination of employment.

VI. Verification

6.1 Bourns' privacy practices are self-certified annually to the U.S. Department of Commerce. The Vice President - Corporate Administration is responsible for:

6.1.1 Ensuring that the privacy guidelines, programs, procedures, training and other measures necessary to implement the Privacy Policy are developed and put into practice;

6.1.2 Overseeing responses to inquiries and resolutions of complaints relating to the privacy of Identifiable Persons;

6.1.3 Working with Bourns' legal department to ensure Bourns' ongoing compliance with applicable privacy laws and agreements, as well as any obligations Bourns may enter into voluntarily, such as the Safe Harbor Principles; and

6.1.4 Overseeing annual assessments of Bourns internal practices to ensure that they conform to the Privacy Policy and related company obligations.

VII . Exhibits

N/A

* * * * *

Bourns Privacy Policy
CEP 1.1700

Corporate Executive Procedure
CEP 1.1700

Bourns Policy on Data Protection and Privacy of Personal Information

Effective Date: 1/9/04 Supersedes: New

John J. Halenda, President Bourns Electronics / Corporate Executive VP