



Policy Number: CORP - 11

Effective: April 1, 2014

Global

US Only

Other _____

SAFE HARBOR PRIVACY POLICY

PURPOSE

Stepan Company ("Stepan") places high importance on earning and keeping the trust of individuals who share their Personal Information with us. In an effort to comply with all applicable privacy and data protection laws, Stepan has certified that it abides by the Safe Harbor privacy principles as set forth by the U.S. Department of Commerce in connection with the collection, storage, use, transfer and other Processing of Personal Information of Employees transferred from the European Economic Area ("EEA") to the United States.

Stepan's Safe Harbor certifications can be found at <http://safeharbor.export.gov/list.aspx>. For more information about the Safe Harbor privacy principles, please visit the U.S. Department of Commerce's Web site at <http://www.export.gov/safeharbor>.

RESPONSIBILITIES OF STEPAN EMPLOYEES

All Stepan businesses and functions are required to review their data practices in light of this Policy and establish and maintain procedures to implement this Policy.

All employees of Stepan are required to comply with all applicable privacy and data protection laws, this Policy and all related Stepan procedures.

DEFINITIONS

The following terms used in this Policy are defined as follows:

"*Affiliate*" means any entity located in the EEA that is controlled, directly or indirectly, by Stepan.

"*Employee*" means any natural or legal person (to the extent a legal person is subject to national data protection law) acting in the capacity of a former, current, or prospective employee, agent, consultant or contractor of Stepan or any of its Affiliates.

"*Personal Information*" means any information that is transferred from the EEA to Stepan in the United States and that relates to an identified or identifiable Employee located in the EEA.

"*Processing*" of Personal Information means doing anything with Personal Information, whether or not by automatic means, such as collecting, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, accessing or providing access to, combining, erasing, or destroying Personal Information.

PRIVACY PRINCIPLES

Although privacy and data protection laws vary from country to country, those of the EEA are based on the following privacy principles. Accordingly, to assure compliance with all applicable data protection laws with respect to Personal Information, as that term is defined in this Policy, and to achieve consistency across the organization, Stepan will adhere to the following privacy principles to the extent required by applicable law with respect to Personal Information of Employees in the EEA:

Limitations on the Collection, Use and Disclosure of Personal Information

- *Notice and Consent* – We will collect and process Personal Information fairly and lawfully, and where appropriate, with the knowledge and/or consent of the data subject in the EEA. The type of notice or consent required will depend on the context and the circumstances, the sensitivity of the Personal Information, the data subject’s reasonable expectations, and legal requirements. Stepan may rely on its Affiliates based in the EEA to provide appropriate notice to Employees in the EEA whose Personal Information is transferred to the United States.
- *Specific Purpose* – We will collect and process Personal Information of Employees in the EEA only for specified, limited and legitimate purposes.
- *Limitations on Use* – We will not process Personal Information in a manner inconsistent with the purposes for which it was originally collected without first obtaining consent of the data subject in the EEA. The type of consent required will depend on the context and the circumstances, the sensitivity of the Personal Information, the data subject’s reasonable expectations, and legal requirements. Stepan may rely on its Affiliates based in the EEA to provide Employees in the EEA with a choice as to whether their Personal Information may be used for a purpose that is inconsistent with the purposes for which the information was originally collected or subsequently authorized by the individual.
- *Data Proportionality* – The Personal Information we collect from Employees in the EEA will be relevant, adequate and not excessive for the purposes for which it is collected or to which the data subject subsequently consents.
- *Transfers to Third Parties*
 - We will disclose Personal Information of Employees in the EEA to third parties (including our Affiliates) only for purposes consistent with those for which the Personal Information was originally collected or to which the data subject has subsequently consented. For example, we may disclose Personal Information of Employees in the EEA to third parties we have retained to perform services on our behalf. Stepan will require service providers to whom it discloses Personal Information of Employees in the EEA, and who are not subject to laws based on the EU Data Protection Directive, to either certify to the Safe Harbor privacy principles or contractually agree to provide at least the same level of protection for Personal Information for Employees in the EEA as is required by the Safe Harbor privacy principles.
 - Before we transfer Personal Information to a third party to use for its own marketing purposes, we will obtain consent of the data subject in the EEA. The data subject’s consent may be express or implied, “opt-out” or “opt-in,” depending on the circumstances and legal requirements. Stepan may rely on its Affiliates based in the

EEA to provide data subjects in the EEA with a choice as to whether their Personal Information may be transferred to a third party for its own marketing purposes.

- There may be exceptions to these general rules, depending on applicable law, if, for example, Stepan believes the disclosure is required by court order, to comply with a law, to prevent a crime, or to enforce a legal right. Stepan also reserves the right to transfer Personal Information of Employees in the EEA in the event the Company sells or transfers all or a portion of its business or assets. If such a sale or transfer occurs, Stepan will use reasonable efforts to direct the transferee to use Personal Information of Employees in the EEA in a manner that is consistent with this Policy. Following such a sale or transfer, Employees the EEA may contact the entity to which Stepan transferred their Personal Information with any inquiries concerning the Processing of that information.

Management of Personal Information

- *Quality* – We will take appropriate steps to ensure that Personal Information of Employees in the EEA is reliable for its intended use and accurate, complete, and current. Stepan may depend on Employees in the EEA to update and correct their Personal Information. Stepan may also rely on its Affiliates in the EEA to take reasonable steps to ensure that the Personal Information of Employees in the EEA with whom they have a direct relationship are reliable for their intended use and are accurate, complete, and current.
- *Access* – We will maintain procedures to give data subjects in the EEA appropriate access to their Personal Information and, when appropriate, an effective means to have their Personal Information corrected, amended, or deleted. Stepan may limit or deny access of employees in the EEA to their Personal Information where providing such access is unreasonably burdensome or expensive under the circumstances, or as otherwise permitted by the Safe Harbor privacy principles. In circumstances in which Stepan receives Personal Information about Employees in the EEA with whom it does not have a direct relationship, its Affiliates in the EEA may be responsible for providing such Employees with access to the Personal Information and the right to correct, amend, or delete the information where it is inaccurate.
- *Security* – We will implement reasonable administrative, physical and technological security measures to protect Personal Information of Employees in the EEA from unauthorized access, unauthorized use, and unauthorized or accidental destruction, modification or disclosure. We will provide a level of security appropriate to the risks and the sensitivity of the Personal Information of Employees in the EEA.
- *Retention* – We will not keep Personal Information of Employees in the EEA in a form that permits identification of data subjects for longer than is necessary for the purposes for which it was collected or to which the data subject has consented, except for legitimate purposes permitted by law, such as regulatory compliance.

Accountability and Enforcement

- *Accountability* – We will designate at least one individual within Stepan to be accountable for compliance with privacy and data protection laws applicable to Employees in the EEA, this Policy and related procedures.

- *Enforcement* – We will provide internal controls for verifying compliance with privacy and data protection laws applicable to Employees in the EEA, this Policy and related procedures.
- *Complaint Process* – We will provide a fair process for investigating and resolving complaints and objections regarding our data practices with respect to Employees and Affiliates in the EEA.

Employees in the EEA may file a complaint concerning Stepan's processing of their Personal Information using the contact information below. Stepan will take steps to remedy any issues arising out of a failure to comply with the Safe Harbor privacy principles. If the complaint cannot be resolved through our internal processes, Stepan will cooperate in investigations by and comply with the advice of competent authorities in the EEA.

In circumstances in which Stepan receives Personal Information about Employees in the EEA with whom Stepan does not have a direct relationship, data subjects may submit complaints concerning the Processing of their Personal Information to the relevant Stepan Affiliate in the EEA, in accord with the Affiliate's dispute resolution process. Stepan will participate in this process at the request of the Affiliate or data subject in the EEA. If the complaint cannot be resolved through the Affiliate's internal processes, the Employee in the EEA may submit the complaint to the state or national data protection or labor authority in the EEA jurisdiction where the Employee works.

Alternatively, and in the Employee's sole discretion, the Employee may wish to resolve his/her complaint with the EU Data Protection Authorities ("DPAs") to serve as an independent recourse mechanism for dispute resolution. The DPAs may propose any appropriate remedy pertaining to the Personal Information of the Employee who has brought the complaint.

AMENDMENTS

This Policy may be amended from time to time consistent with the requirements of the Safe Harbor privacy principles. We will post any revised policy on this Web site.

CONTACT INFORMATION

To contact Stepan about questions or concerns about this Policy or Stepan's practices concerning Personal Information of Employees in the EEA, either Submit a General Inquiry at www.stepan.com or you may write to us at:

Sr. Manager Corporate Human Resources
Stepan Company
22 W. Frontage Road
Northfield, Illinois 60093

The Company reserves the right to amend or alter the Safe Harbor Privacy Policy or other Company policies at any time for any reason. This Safe Harbor Privacy Policy or any other Company policy is not an employment contract between the Company and any of our employees, officers or directors and does not alter the Company's policy of at-will employment.