



Data Privacy Framework Policy

Concerning personal data transferred from the European Economic Area (“EEA”)¹ and Switzerland to the United States of America (“U.S.”)

1. Introduction

The U.S. Department of Commerce and the European Commission as well as Switzerland have agreed on a framework of data protection principles and supplemental principles to enable U.S. companies to provide an adequate level of protection for personal data transferred from the EEA to the U.S. (“EU-U.S. Data Privacy Framework” / “Swiss-U.S. Data Privacy Framework”; together the “Data Privacy Framework”). Inteva Products, LLC (“Inteva”) respects the privacy of its customers, business partners and employees and recognizes the need for appropriate protection and management of personal information provided. Inteva on behalf of itself and its wholly owned U.S. domiciled entities, has made a decision to voluntarily adhere to the Data Privacy Framework Principles recognized by the EEA and Switzerland as providing adequate data protection. Inteva complies with the Data Privacy Framework as agreed upon between the U.S. Department of Commerce and the European Commission and Switzerland regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Inteva has certified that it adheres to the Data Privacy Framework Principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, recourse, enforcement and liability as well as the supplemental principles of the framework. To learn more about the Data Privacy Framework program, please visit <https://www.dataprivacyframework.gov/>. A current list of organizations certified under the Data Privacy Framework (“Data Privacy Framework List”) is available at <https://www.dataprivacyframework.gov/s/participant-search>.

Should there be any conflict between the Data Privacy Framework principles and this Data Privacy Framework Policy (“Policy”), the Data Privacy Framework principles will prevail.² This Policy outlines the general practices for implementing the requirements of the Data Privacy Framework in connection with personal data that is transferred from the EEA and Switzerland to the U.S.: including the types of information that is collected and transferred; how it is used; and, the choices individuals located in the EEA and Switzerland have regarding the use of, and their ability to correct, that information.

2. Scope

This Policy applies to all Inteva U.S. operations, divisions and subsidiaries as far as personal information from the EEA or Switzerland is received in any format whatsoever, including electronic,

¹ The EEA currently includes the following countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Iceland, Liechtenstein, and Norway.

² Information about the U.S. Department of Commerce Data Privacy Framework certification can be found at <https://www.dataprivacyframework.gov/>.



paper or oral transmission. This Policy also applies to Agents (defined below) that handle and process EEA and/ or Swiss personal data on behalf of Inteva.

3. Definitions

For purpose of this Policy, the following definitions shall apply:

“Agent” means any third party processor that collects and/or uses personal information provided by Inteva to perform tasks on behalf of and under the instructions of Inteva.

“Personal Data” and **“Personal Information”** are data about an identified or identifiable individual that are within the scope of the Regulation (EU) 2016/679 (General Data Protection Regulation) or the Swiss Federal Act on Data Protection, received by an organization in the United States from the European Union or Switzerland, and recorded in any form. Personal information does not include information that is anonymous (e.g. statistical information not relating to an identifiable person).

“Sensitive Personal Information” means personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual or personal information received from a third party that is identified and treated as sensitive by the third party. Where Swiss individuals are concerned, “Sensitive Personal Information” also includes ideological views or activities and information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

“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.

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

4. Processing of EEA and/ or Swiss personal data

Inteva may from time to time process certain EEA and/ or Swiss Personal Information about current or prospective customers, business partners, suppliers, vendors, service providers, independent contractors, consumers, E-mail- users, selected test users, employees and candidates for employment, including information recorded on various media as well as electronic data. Inteva will process these data in conformity with the Data Privacy Framework Principles and will continue to apply the Principles to personal data received under the application of the Data Privacy Framework .

Inteva will use Personal Information concerning business partners and customers to provide customers and business partners with information and services and to help Inteva personnel better understand the needs and interests of these business partners and/or customers. Specifically, Inteva uses information to maintain and protect Inteva data confidentiality, integrity, and availability, to help customers and business partners complete a transaction or order, to facilitate communication, to deliver products/services, to provide customers and business partners with information and services, to bill for purchased products/services, to submit legal bills, to provide ongoing service and support, for the hiring process, to select service and personnel, to communicate to individuals about products, services and related issues, to provide access to the systems, to facilitate Inteva’s internal administrative purposes, to book travel, accommodation and event registration, for business continuity and/or disaster

recovery, for direct marketing, for product design collaborative and concurrent engineering, to organize and manage joint projects and joint ventures, to maintain, administer and to comply with Inteva's legal, regulatory compliance and auditing obligations, policies and procedures, to deliver IT services, for network management and data repository replication, to prevent computers from running unknown programs, including malware, providing logs for after-the-fact remediation in case of a security break on the computer and information security investigations and forensics. Occasionally Inteva personnel may use Personal Information to contact customers and business partners to complete surveys that are used for quality assurance purposes.

Inteva may also share Personal Information with its service providers and suppliers (Agents) for the sole purpose and only to the extent needed to support the customers' business needs. Service providers and suppliers are required to keep confidential Personal Information received from Inteva and may not use it for any purpose other than originally intended. In case of data transfers to third parties acting as controllers the affected individuals will be informed about the transfer and the underlying purposes respectively.

Inteva also collects Personal Information concerning its employees (Human Resources Data) in connection with administration of its Human Resources programs and functions and for purpose of communicating with its employees. Inteva also applies the Data Privacy Framework Principles to these data. Further information in this regard can be found in Inteva's Human Resources Data Privacy Framework Policy available for employees at the Inteva Intranet Library.

5. Privacy Principles

A detailed description of the Data Privacy Framework Principles can be found on the website of the U.S. Department of Commerce.

5.1. Notice

Where Inteva collects Personal Information directly from individuals in the EEA and/ or Switzerland or receives it from its European affiliates, or other third parties, it or the respective European affiliate will inform those individuals about the purposes for which it collects and uses Personal Information about them; the transfer to Inteva in the U.S., the types or identity of third parties acting as controllers to which Inteva discloses that information, the purposes for which it does so; and the choices and means, Inteva offers individuals for limiting the use and disclosure of their Personal Information, and about the right of individuals to access their personal data. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Information to Inteva, or as soon as practicable thereafter, and in any event before Inteva uses the information for a purpose other than that for which it was originally collected or discloses it for the first time to a third party.

5.2. Choice

Inteva will offer individuals the opportunity to choose (opt-out) whether their Personal Information is (a) to be disclosed to a third party acting as a controller, or (b) to be used for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive personal information, Inteva will give individuals the opportunity to



affirmatively and explicitly consent (opt-in) to the disclosure of their Sensitive Personal Information to (a) a third party acting as a controller or (b) the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Inteva will provide individuals with reasonable (especially clear and conspicuous, readily available) mechanisms to exercise their choices.

5.3. Accountability for Onward Transfer

Inteva will transfer Personal Information to Agents only for limited and specific purposes and obtain contractual assurances from its Agents that they will safeguard Personal Information consistent with this Policy and that they will provide at least the same level of protection as is required by the relevant Data Privacy Framework principles. Inteva recognizes its responsibility and potential liability for onward transfers to Agents. Where Inteva has knowledge that an Agent is using or disclosing Personal Information in a manner contrary to this Policy and/or the level of protection as required by the Data Privacy Framework Principles, Inteva will take reasonable and appropriate steps to prevent, remediate or stop the use or disclosure.

If Inteva transfers personal information to non-agent third parties acting as a controller, Inteva will apply the Notice and Choice Principles unless a derogation for specific situations under European or Swiss data protection law applies and will obtain contractual assurance from these parties that they will provide the same level of protection as is required under the Principles.

5.4. Access

Upon request, Inteva will grant individuals reasonable access to Personal Information that it holds about them. In addition, Inteva will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete or has been processed in violation of the Data Privacy Framework Principles. Inteva may limit an individual's access to Personal Information where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy or where the legitimate rights of persons other than the individual would be violated.

5.5. Security

Inteva will take reasonable and appropriate precautions to protect Personal Information in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5.6. Data Integrity and Purpose Limitation

Inteva will use Personal Information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual (see 5.2.). Inteva will take reasonable steps to ensure that Personal Information is relevant to its intended use, accurate, complete, and current. Inteva will adhere to the Principles as long as it retains personal information received under its Data Privacy Framework certification.

5.7. Recourse, Enforcement and Liability

Inteva utilizes the self-assessment approach to assure its compliance with this Policy. Inteva periodically verifies that this Policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented, and in conformity with the Data Privacy Framework principles. Inteva encourages interested persons to raise any concerns with it using the contact information below. Inteva will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Information in accordance with the principles contained in this Policy.

If Inteva determines that any person in its employ is in violation of this Policy such person will be subject to disciplinary action.

Any questions or concerns regarding the use or disclosure of personal information should be directed to the Chief Information Officer at the address given below. Inteva will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with the principles contained in this Policy.

With respect to any complaints relating to this Policy that cannot be resolved through Inteva's internal processes, Inteva has agreed to cooperate with the data protection authorities in the EU and the Swiss Federal Data Protection and Information Commissioner and to participate in the dispute resolution procedures established by these Authorities to resolve disputes pursuant to the Data Privacy Framework principles available at the addresses given below. In the event that Inteva or such Authorities determines that Inteva did not comply with this Policy, Inteva will take appropriate steps to address any adverse effects and to promote future compliance. Inteva is also subject to the investigatory and enforcement powers of the Federal Trade Commission, which is the competent supervisory body under the Data Privacy Framework.

Where a complaint cannot be resolved by any of the before mentioned recourse mechanisms, individuals have a right to invoke binding arbitration under the Data Privacy Framework Panel as recourse mechanism of 'last resort'.

6. Limitations

Inteva's adherence to the Data Privacy Framework Principles may be limited (a) to the extent necessary to meet applicable national security, public interest, or law enforcement requirements, e.g. in the course of lawful requests by public authorities (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the General Data Protection Regulation or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts.

7. Contact Information



Questions or comments regarding this Policy should be submitted to Inteva by mail or e-mail as follows:

ATTN: Dennis Hodges, CIO
Inteva Products, LLC
Address: 1401 Crooks Road, Troy, MI 48084-7106
Phone: 1 (248) 655-0650
Fax: 1 (866) 914-3142
E-Mail: dhodges@intevaproducts.com

If you are a citizen of an EEA member state, you may also [address any unresolved complaints](#) by contacting your local Data Protection Authority at the following address:

https://edpb.europa.eu/about-edpb/board/members_en

If you are a citizen of Switzerland, [unresolved complaints can be addressed](#) to the Swiss Federal Data Protection and Information Commissioner at the following address:

<https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/kontakt.html>

8. Changes to this Policy

This Policy may be amended from time to time, consistent with the requirements of the Data Privacy Framework principles. Appropriate public notice will be given concerning such amendments.

Effective Date: September 26, 2023