

Cerence Global Trade Compliance Policy

Purpose

The purpose of this policy is to establish and communicate expectations for compliance with the laws and regulations governing the export and import of goods, software and technologies in all jurisdictions in which Cerence operates.

Scope

This Global Trade Compliance Policy is applicable to all of Cerence, its subsidiaries or affiliated companies staff members, consultants and contract workers worldwide ("Covered Persons").

Policy Statement

It is the policy of Cerence to fully comply with all applicable import and export laws and regulations, including but not limited to the U.S. Export Administration Regulations (EAR), International Traffic in Arms regulations (ITAR), Department of Treasury Office of Foreign Asset Control (OFAC), Customs and Border Patrol (CBP) as well as other applicable country specific laws and regulations governing the export and import of products, services and technologies.

As a U.S. company, Cerence must comply with U.S. export control laws in all countries we conduct business in as well as local, country specific laws.

Trade Compliance Guidelines

I. Product export classification and part number creation

All products and technology must be classified with an Export Control Classification Number (ECCN) prior to being exported or sold. ECCNs are a 5-digit alpha-numeric code used to determine export restrictions and government license requirements. The product manager shall contact the Legal Department 60 days prior to requesting part numbers to obtain their product's ECCN. When submitting the request for part numbers to be created the product manager shall provide the ECCN supplied by the Legal Department to the part number creation team. The part number creation team will assign the ECCN to the part number upon creation in the Cerence ERP system.

II. What everyone needs to know about their export transaction and sale to comply with the law:

- a. Know **what product** is being sold and/or exported. Some voice biometrics products have an ECCN of 3D980, are controlled for crime control purposes, are highly regulated, can't be sold to China and require a U.S export license when being sold to many other countries.
- b. Know **where** the product is going. Some countries and regions are sanctioned and Embargoed. Cerence currently restricts direct and indirect business with Cuba, Iran, Sudan, Syria, North Korea and the Crimean region of the Ukraine/Russia.
- c. Know **your customer** and **end user**. Many countries, even those that are friendly and considered allies, have entities and individuals like terrorists and drug cartel that governments have sanctioned making it illegal for Cerence conduct business with.
- d. Know what Cerence's products are being **used for**. Export regulations worldwide restrict the use of products with or in support of nuclear or missile technology, chemical and biological weapons, maritime nuclear propulsion, military uses or weapons of mass destruction.
- e. Know and be on the lookout for **Red Flags**. A red flag is something about a transaction that is unusual or out of the ordinary and can be an indication Cerence's product could be destined for a restricted end use, restricted end user, or restricted country or region. As an example, a small mom and pop bakery seeking to purchase advanced voice biometrics products that are typically sold to and used by intelligence agencies is a red flag. The product and its technology don't align with the end user's business which could be an indication they are a front company purchasing for another party with the intent to divert the product to a restricted end user, restricted end use or restricted destination.

If a red flag, restricted party, restricted end use or sanctioned country is encountered the transaction must be stopped and escalated to the Legal Department

III. Anti-boycott

Anti-boycott regulations prohibit Cerence from supporting any non-U.S. sanctioned boycott. The most common non-U.S. sanctioned boycott is the Arab League boycott of Israel. Prohibited conduct includes:

- Agreements to refuse or actual refusal to do business with or in Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality.
- Agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies.
- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person.

Requests to comply with a non-U.S. sanctioned boycotts must be denied and escalated to the Legal Department

IV. Importing into the U.S. and other countries globally

The U.S. and other countries have customs rules and import laws that govern the movement of product into their territory. Covered Persons must provide accurate documentation, appropriate country of origin on product and documents, accurate Harmonized Tariff Schedule (HTS) classification of goods and make proper declarations on the quantity and value of product being imported.

V. Record Retention

Import and Export records must be retained for a minimum of five years or in accordance with specific Cerence record retention policies or country specific requirements if longer than five years.

VI. Reporting Violations

Any Covered Person who has knowledge that a violation of the regulations or this policy is about to occur or has occurred should promptly report the matter to the Legal Department at generalcounsel@cerence.com. Employees may also report suspected violations through Cerence's anonymous whistleblower hotline via the Internet at <https://www.whistleblowerservices.com/cerence> or via telephone at +1 855-833-8043. In accordance with Cerence's Whistleblower Policy, reports of violations will be kept confidential to the extent possible, and Cerence will not retaliate against reporting individuals for good faith reports.

Disclaimer

Nothing herein is intended to constitute a contract between Cerence and any employee and Cerence reserves the right to revise or terminate this Policy at any time. All Cerence employees are expected to comply with all Company policies and the failure to do so may result in remedial action by Cerence as permitted by applicable agreements and law. Nothing in this Policy should be construed to limit employees' rights to engage in protected whistleblower activity or concerted activity under Section 7 of the U.S. National Labor Relations Act.