Arnold & Porter

ATTORNEY WORK PRODUCT
PRIVILEGED & CONFIDENTIAL

Memorandum

To: Syensqo SA

From: Arnold & Porter Kaye Scholer LLP

Date: October 30, 2024

Re: U.S. Export Control Analysis Regarding Use of a EU-based Data Storage System

---

Syensqo SA ("Syensqo" or the "Company") has asked us to provide an analysis of digital storage requirements of data subject to U.S. export controls under applicable U.S. export control laws, including the Export Administration Regulations ("EAR"), 15 C.F.R. Parts 730-774 and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-130. We understand that Syensqo is considering transferring certain EAR- and ITAR-controlled data to a global instance of SAP SE ("SAP")'s SAP s/4HANA located in the European Union (EU).[1]

In sum, the Company may store data subject to U.S. export controls in the EU, provide certain requirements are met. That said, the Company should take certain steps to mitigate the risks of inadvertent violations of U.S. law in connection with such data storage, as outlined below.

Section I of this memorandum presents the relevant facts and assumptions. **Section II** provides overview of the key applicable legal frameworks under U.S. law. Our analysis, conclusions, and recommendations are provided in **Section III**.

[1] This analysis is limited to applicable data requirements under U.S. export controls. This memorandum does not address other potentially applicable requirements under U.S. law, including cybersecurity requirements under certain U.S. governmental contracting regulations.

I. FACTS AND ASSUMPTIONS

The following are the facts that we understand based on the information that Syensqo has provided to us, as well as certain additional assumptions we have made. Should any of the facts or assumptions change, our analysis may change.

- Syensqo's Composite Materials business in the United States manufactures products that are subject to EAR and ITAR export controls for items and technologies.
- Accordingly, we understand the Company currently stores certain data subject to the EAR and the ITAR in a U.S.-based SAP instance.
- The Company is considering migrating the U.S. data from its U.S.-based SAP instance to a global SAP s/4HANA instance, located in the EU.
- Following migration, access to the U.S. data will be limited to "U.S. persons" of U.S. companies, unless otherwise authorized by a license authorization or license exception, where applicable.

II. RELEVANT LEGAL FRAMEWORKS

Nearly all items subject to U.S. export restrictions are regulated by one of two U.S. regimes. Specifically, the EAR, which is administered by BIS, regulates the export of commercial products generally, including "dual-use" commercial items. Dual-use items subject to the EAR have predominantly commercial uses, but can also have military applications. In contrast, the ITAR governs the export and temporary import of military items, referred to as "defense articles," which are described on the U.S. Munitions List. The applicable provisions of these regulatory regimes are summarized below.

A. The EAR

The EAR regulates the export, reexport, and transfer in country of "items" that are "subject to the EAR." The term "item" under the EAR refers to "commodities, software, and technology."[2] A "commodity" is "[a]ny article, material, or supply except technology and software." "Technology" is any "[i]nformation necessary for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing . . . of an item." "Technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media

[2] 15 C.F.R. Part 772.

or information revealed through visual inspection of an item. "Software" generally includes any machine readable object code, as well as, in some cases, source code, although the regulations sometimes treat source code as a form of "technology."

Licensing and other requirements under the EAR apply only to the extent the item at issue is "subject to the EAR," meaning the item falls within the jurisdictional scope of the EAR. Under the EAR, the terms export, reexport, and transfer are defined as follows:

Export (15 C.F.R. § 734.13)

(1) An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;

(2) Releasing or otherwise transferring "technology" or source code (but not object code) to a foreign person in the United States (a "deemed export");

(3) Transferring by a person in the United States of registration, control, or ownership of:

(ii) A spacecraft subject to the EAR that is not eligible for export under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country; or

(iii) Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country.

Reexport (15 C.F.R. § 734.14)

(1) An actual shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;

(2) Releasing or otherwise transferring "technology" or source code subject to the EAR to a foreign person of a country other than the foreign country where the release or transfer takes place (a deemed reexport);

(3) Transferring by a person outside the United States of registration, control, or ownership of:

(i) A spacecraft subject to the EAR that is not eligible for export under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country; or

(ii) Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country.

In-country Transfer (15 C.F.R. § 734.16)

A transfer (in-country) is defined under the EAR as a change in end use or end user of an item within the same foreign country. Transfer (in-country) is synonymous with In-country transfer.

Depending on the relevant classification of an item subject to the EAR, a license authorization issued by the U.S. department of the Commerce or use of an applicable license exception may be required prior to the export, reexport, or transfer (in-country) of the item.

B. The ITAR

The ITAR regulates the export and temporary import, as well as the manufacture and brokering, of "defense articles," including items and "technical data," which are designated on the U.S. Munitions.[3] The ITAR also regulates re-exports and re-transfers, which involve the transfers of defense articles, technical data, or defense services from one foreign country or foreign person to another foreign country or foreign person.[4]

Under the ITAR, the terms export, reexport, and retransfer (*i.e.*, in-country transfer) are defined as follows:

Export (22 C.F.R. § 120.50)

[3] *See* 22 C.F.R. § 120.2.

[4] The ITAR also regulates "defense services" provided to foreign persons in connection with, among other things, the design, development, manufacture, use, maintenance, modification, repair, or destruction of "defense articles." Furnishing controlled technical data to foreign persons and providing military training to foreign units and forces are examples of defense services.

(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;

(2) Releasing or otherwise transferring technical data to a foreign person in the United States (a deemed export);

(3) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to this subchapter by a U.S. person to a foreign person;

(4) Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;

(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or

(6) The release of previously encrypted technical data as described in 22 C.F.R. § 120.56(a)(3) and (4).

Reexport (22 C.F.R. § 120.51)

(1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;

(2) Releasing or otherwise transferring technical data to a foreign person who is a citizen or permanent resident of a country other than the foreign country where the release or transfer takes place (a deemed reexport); or

(3) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to this subchapter between foreign persons.

In-country Transfer (22 C.F.R. § 120.52)

(1) A change in end-use or end-user, or a temporary transfer to a third party, of a defense article within the same foreign country; or

(2) A release of technical data to a foreign person who is a citizen or permanent resident of the country where the release or transfer takes place.

Absent very narrow circumstances, a license authorization issued by the U.S. Department of State is required prior to the export, reexport, or transfer (in-country) of technical data subject to the ITAR.

C. Activities that Are Not Exports, Reexports, or Transfers

Under both the EAR and the ITAR there is an exception for data that is sent, taken, or stored to or within certain locations provided certain requirements are met. This exception is sometimes referred to as the "encryption" or "cloud" exception. Specifically, under EAR Section 734.18(a)(5), the following is **not** considered an export, reexport, or retransfer:

(5) Sending, taking, or storing "technology" or "software" that is:

(i) Unclassified;

(ii) Secured using 'end-to-end encryption;'

(iii) Secured using cryptographic modules (hardware or "software") compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by "software" implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other equally or more effective cryptographic means; and

(iv) Not intentionally stored in a country listed in Country Group D:5 (*see* supplement no. 1 to part 740 of the EAR) or in the Russian Federation.

Similarly, under ITAR Section 120.54(a)(5), the following is **not** considered an export, reexport, or retransfer:

(i) Unclassified;

(ii) Secured using 'end-to-end encryption;[5]

[5] (1) For purposes of this section, end-to-end encryption is defined as:

(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128);

(iv) Not intentionally sent to a person in or stored in a country proscribed in 22 C.F.R. § 126.1 or the Russian Federation;[6] and

(v) Not sent from a country proscribed in 22 C.F.R. § 126.1 or the Russian Federation.

Notwithstanding the above, the provision of access information (*e.g.*, user credentials) may result in the export of technology (under the EAR) or technical data (under the ITAR), even if the above encryption requirements have been met.[7] Traditionally, the U.S. Department of Commerce has taken the position that the mere theoretical access to EAR-controlled technology does not trigger EAR licensing requirements. In contrast, the U.S. Department of State views the ability to access technical data as an export, reexport, or transfer (in-country), even if the relevant technical data is not actually accessed.

III. ANALYSIS

As noted above, a prior license authorization may be required to export, reexport, and/or transfer data controlled under the EAR or the ITAR. Here, the transmission of the data to the EU SAP instance itself would be considered a "transmission" out of the United States—*i.e.*, an export. Further, the receipt of the data by SAP and/or the Company's operations outside of the U.S. may involve transfer activities controlled under the EAR or the ITAR. Accordingly, Syensqo may not be able to transfer its current US-based SAP system to SAP or another a EU-based system without seeking the U.S. government's approval.

(i) The provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and
(ii) The means of decryption are not provided to any third party.
(2) The originator and the intended recipient may be the same person. The intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, such as by a license or other approval pursuant to this subchapter.

[6] Note that this is outdated as Russia is now a 126.1/D:5 country.

[7] See 15 C.F.R. § 734.15(b); 22 C.F.R. § 120.56.

To the extent, however, that all relevant data is sent from the U.S. in an encrypted format to be stored in the SAP s/4HANA system in the EU, then if it otherwise met the encryption exception criteria above, SAP, as well as the territory of its servers outside the United States, would not need to be authorized (provided no portion of the data is stored on servers or other equipment located in a 126.1/D:5 country). Stated differently, no license authorization would be required because the data would not be exported, reexported, or transferred under applicable U.S. law.

A few caveats. First, a license authorization may be required to the extent that the U.S. data stored on SAP s/4HANA is accessed abroad. For example, if an employee of one of the Company's U.S.-based companies accesses export controlled information while travelling abroad, a license authorization may be required. While there are certain exceptions for U.S.-based employee travel, appropriate compliance steps are required to confirm if an applicable exception will apply. Therefore, we recommend that no U.S. employees access U.S. export control information stored on SAP s/4HANA, unless the Company's compliance personnel have cleared the employee's access beforehand.

Second, the access would need to be protected at the encryption standards identified above. The basic operational principle for both the ITAR and the EAR is that any non-U.S. person must be authorized prior to accessing any ITAR or EAR controlled data. As a result, the default rule is that any ITAR or EAR controlled data must only be accessible to those individuals that are confirmed to be authorized for access to such data (whether because no license is required, an exception applies, or a specific authorization applies). Therefore, the Company should take steps to ensure that access to U.S. export controlled data is limited to U.S. persons employees of U.S. companies, and that the data is otherwise segregated from and/or inaccessible to users outside of the United States.

Third and relatedly, an reexport/retransfer of ITAR-controlled technical data occurs as a result of the provision of "access information" for such technical data even if it is never actually accessed. In the context of IT and other third-party service providers, this means that all employees that *can* access data must be appropriately authorized. Accordingly, the Company should confirm that no Company employee, consultant, etc. and no SAP employees, consultant or other third parties have the ability to access the U.S. data stored on SAP s/4HANA, even if such access related to the provision of system troubleshooting or other technical assistance. This last requirement has proven especially challenging for other companies. Essentially the ability to store the data outside the U.S. is contingent on no non-U.S. person and no-non-U.S. entity being able to access the data while it is stored outside the U.S. IT service providers, whether internal or external, frequently want the ability to access the data for troubleshooting, repairs, etc. but if they are given access to the encryption keys, whether or not they actually access the data, there may be a violation.

* * *

This memorandum provides an analysis under U.S. law and no other laws, and is based on the U.S. export controls as of the date of this memorandum.