Westlaw Today
powered by Reuters

Ten takeaways from SAP's recent export controls and economic sanctions settlement agreements

By Mario Mancuso, Esq., Sanjay Mullick, Esq., Anthony Rapa, Esq., and Abigail Cotterill, Esq., Kirkland & Ellis LLP

MAY 14, 2021

On April 29, 2021, the U.S. Commerce Department's Bureau of Industry and Security[1] ("BIS"), the U.S. Department of the Treasury's Office of Foreign Assets Control[2] ("OFAC"), and the U.S. Department of Justice[3] concurrently announced settlement agreements with Germany's SAP SE ("SAP"), which agreed to pay over $8 million in penalties for transactions with Iran in violation of U.S. export controls and economic sanctions.

Though significant, the penalties were mitigated by SAP being the first[4] company to avail itself of DOJ's Export Control and Sanctions Enforcement Policy for Business Organizations.[5]

SAP filed voluntary self-disclosures with DOJ, BIS, and OFAC, resulting in reduced penalties as well as a Non-Prosecution Agreement with DOJ (the "NPA"). The settlements offer several important lessons for technology companies conducting global transactions.

Software

1. Commercial items can have national security implications. At issue was the unauthorized download of U.S.-origin business enterprise software, including certain products implementing encryption functionality.

Though such software is used worldwide for normal applications, the export or reexport to Iran of U.S.-origin software generally is prohibited. OFAC stated that SAP's exportation of such software and services to be used by Iranian businesses "caused harm to U.S. sanctions program objectives and undermined U.S. policy objectives."

2. Software-related violations can multiply quickly. OFAC indicated that within a five-year period, SAP authorized 13 sales of SAP software licenses and 169 sales of related maintenance services and updates from the United States in violation of U.S. sanctions on Iran.

According to BIS, these original authorizations then resulted in end-users in Iran making over 24,000 downloads of SAP software products. This figure includes upgrades and patches, which companies routinely make available under software agreements, but which each count as a separate export.

Technology

3. Software as a Service ("SaaS") may be considered exports under U.S. law. In addition to the prohibited software downloads, SAP also made unauthorized sales of cloud-based software subscription services to entities that shared access to those services with Iranian customers and employees.

Through the cloud, the servers hosting the software actually were located in the United States. However, under software subscription services, SAP's customers in third countries and ultimately users in Iran could access and retrieve those applications.

Though significant, the penalties were mitigated by SAP being the first company to avail itself of DOJ's Export Control and Sanctions Enforcement Policy for Business Organizations.

4. Leverage technology tools for compliance purposes. OFAC pointed out that SAP did not screen customers' Internet Protocol (IP) addresses identifying the country in which its software was downloaded. OFAC emphasized that SAP did not employ these measures, though knowing its U.S.-based content delivery provider had this ability. IP screening could have verified the geolocation of users making download requests and safeguarded against prohibited transactions.

Diligence

5. Don't ignore what you learn. OFAC explained that a 2006 internal audit found that SAP was not conducting IP geolocation screening, exposing SAP to sanctions risk. Nonetheless, even though this "compliance vulnerability" subsequently was brought to the attention of SAP's Executive Board, it was not until 2015 that SAP implemented it.

Under OFAC's Economic Sanctions Enforcement Guidelines,[6] which determine penalty disposition, disregard for warning signs

and failure to take corrective action generally are considered aggravating factors.

6. Make appropriate efforts to know your counterparties. According to OFAC, SAP at times sold the software and services through third-party resellers located in Europe, Asia, and the Middle East, but did not conduct sufficient diligence on them.

DOJ pointed out that some of these partners distributed the software to "pass-through entities," including Iranian-controlled "front companies" and "shell entities," that provided the software to users in Iran. OFAC indicated that SAP has since implemented a protocol whereby a third-party auditor reviews SAP's partners' proposed sales.

Compliance

7. Timely integrate acquisitions into your compliance infrastructure. OFAC explained that starting in 2011, SAP began to acquire several U.S.-based cloud business subsidiaries that operated internationally. Though SAP was aware from transaction diligence that many of these entities did not have export controls and sanctions compliance programs, it did not fully integrate them into its own compliance structure until 2017.

Under OFAC's Economic Sanctions Enforcement Guidelines, which determine penalty disposition, disregard for warning signs and failure to take corrective action generally are considered aggravating factors.

In the interim, according to OFAC, they operated with technological shortcomings and at times without viewing sanctions compliance as necessary, resulting in the circumstances under which the transactions with Iran occurred.

8. Ensure management engagement. DOJ stated that while for years SAP's audit reports identifying its compliance shortfalls were provided to SAP's senior managers, board members, U.S. Legal Counsel responsible for export controls, and Head of Logistics, SAP did not take remedial action.

Under OFAC's Framework for OFAC Compliance Commitments,[7] its industry guidance on sanctions compliance programs (SCP), senior management is to expressly review and approve an organization's SCP. Consistent with this, the DOJ NPA requires SAP's Executive Board to communicate that it has reviewed and endorses SAP's export controls and sanctions training program.

Cooperation

9. Consider voluntary self-disclosure. OFAC indicated that the applicable statutory maximum civil monetary penalty was over $56 million, but that it arrived at a settlement amount of just over $2 million (deemed satisfied so long as SAP paid a greater amount due to DOJ) in part because SAP voluntarily disclosed the conduct.

DOJ also emphasized SAP's voluntary disclosure and significant cooperation in its decision not to file criminal charges, even though certain SAP leaders and executives knew from whistleblower complaints and public information that SAP's third party resellers had business ties to Iranian companies, and that the front companies planned to use SAP's software in Iran.

10. The U.S. government has penalty levers beyond fines. The BIS settlement agreement requires that for three years SAP conduct an annual internal audit of its export controls compliance program and report its findings.

BIS has made this a condition of the "granting, restoration, or continuing validity of any export license, license exception, permission, or privilege granted, or to be granted, to SAP," and the NPA requires SAP to provide copies of the audit reports to DOJ, as well.

The U.S. government's ability to cut off access to U.S. technology is a key reason why U.S. and non-U.S. companies take export controls compliance seriously.

Notes

[1] https://bit.ly/3vZxSR5

[2] https://bit.ly/3y6r5qt

[3] https://bit.ly/3hoKPzC

[4] https://bit.ly/3y8g3kD

[5] https://bit.ly/3y3LRY1

[6] https://bit.ly/2SNvbDT

[7] https://bit.ly/3w6NH8n

About the authors




(L-R) **Mario Mancuso** is a partner at **Kirkland & Ellis LLP** and leads the firm's International Trade and National Security Practice. He focuses on guiding private equity sponsors and companies through the Committee on Foreign Investment in the United States process and resolving crises involving economic sanctions and export control-related investigations by the U.S. government. He can be reached at mario.mancuso@kirkland.com. **Sanjay Mullick** is a partner with the firm, focused on representing clients in investigative, regulatory and transactional matters related to economic sanctions, export and import controls, anti-money laundering and anti-corruption. He can be reached at sanjay.mullick@kirkland.com. **Anthony Rapa** is a partner counseling companies and private equity sponsors worldwide regarding economic sanctions and export control issues in the context of corporate transactions and internal investigations. He can be reached at anthony.rapa@kirkland.com. **Abigail Cotterill**, of counsel at the firm, provides legal advice to companies, financial institutions and private equity sponsors on the regulatory and other risks of operating or investing across international borders, with a focus on economic sanctions, export controls and anti-corruption. She can be reached at abigail.cotterill@kirkland.com. All the attorneys are based in the firm's Washington, D.C., office.

This piece was first published on Reuters Legal News and Westlaw Today on May, 14, 2021.