



**U.S. Department of Justice**

**National Security Division**

*Counterintelligence and Export Control Section*

*Washington, D.C. 20530*

April 20, 2021

Kwame J. Manley, Esq.  
Robert Luskin, Esq.  
Paul Hastings LLP  
2050 M Street, NW  
Washington, DC 20036

Dear Attorneys Manley and Luskin,

The United States Department of Justice's National Security Division and the United States Attorney's Office for the District of Massachusetts (collectively, "the Offices"), and SAP SE ("SAP" or the "Company"), enter into this Non-Prosecution Agreement (the "Agreement"). The Offices, based on the understandings specified below, will not criminally prosecute the Company for any crimes relating to the conduct described in the Statement of Facts attached hereto as Attachment A (the "Statement of Facts"). The Company, pursuant to authority granted by the Company's Board of Directors, also agrees to certain terms and obligations of the Agreement as described below.

1. The Offices enter into this Agreement based on the following individual facts and circumstances presented by this case and the Company, including:

a SAP received full voluntary self-disclosure credit because it timely and voluntarily disclosed to the Offices the conduct described in the Statement of Facts;

b SAP received full credit for its cooperation with the Offices for its extensive, thorough investigation and real-time cooperation with the Offices to date. SAP conducted a thorough internal investigation, proactively identified issues and facts that would likely be of interest to the Offices, and provided updates to the Offices. The Company made regular factual presentations to the Offices and shared information that would not have been otherwise available to the Offices. SAP voluntarily made foreign-based employees available for interviews in a mutually agreed upon overseas location. It produced documents, including translations, to the Offices from foreign countries in ways that furthered the Offices' investigation. It also provided counsel to employees to facilitate their cooperation. SAP collected, analyzed, and organized voluminous evidence and information for the Offices. And SAP identified, investigated, and disclosed conduct to the Offices that was outside the scope of the Company's initial disclosures;

c SAP timely remediated and implemented significant changes to its export compliance and sanctions program, spending more than \$27 million on such changes, including (1) implementing GeoIP blocking; (2) deactivating thousands of individual users of SAP cloud based services based in Iran; (3) transitioning to automated sanctioned party screening for its cloud businesses; (4) auditing and suspending SAP Partners that sold to Iran-affiliated customers; (5) requiring new acquisitions to adopt GeoIP blocking and requiring involvement of the Export Control team before acquisition; (6) initiating enhanced export control employee training program across the company; (7) terminating employees who were aware of the sale of SAP software to users in Iran; (8) committing to maintain a risk-based export controls compliance program and mandating compliance certifications; and (9) hiring approximately 15 additional professionals devoted exclusively to export control and sanctions compliance;

d SAP has committed to continuing its cooperation with regard to any investigation by the Offices as set forth in paragraph 5 below;

e SAP committed serious offenses that affect the national security of the United States, but the national security ramifications were tempered by SAP's voluntary self-disclosure, remediation, and cooperation; and

f SAP has no history of similar misconduct.

2. In light of the Company's significant remediation efforts and the current state of its export control and sanctions compliance program, the Offices have determined that a Monitor is not necessary. However, the Company is separately under a settlement agreement with the Department of Commerce, Bureau of Industry and Security ("BIS") and the Department of the Treasury, Office of Foreign Assets Control ("OFAC") ("Administrative Agreements"). These Administrative Agreements require audits and certifications that SAP complies with U.S. export laws. SAP will provide the Offices with copies of those audits and certifications, as described below in paragraph 6.

3. As part of this agreement, SAP will be required to pay any unlawfully obtained revenue, as described below. In light of the factors in paragraphs 2(a)-(f) above, however, the Offices will not seek any additional penalty amount.

#### **SAP's Promises and Obligations**

4. In consideration of the Offices' promises and obligations set forth below in paragraph 8, SAP knowingly, voluntarily, and with the advice of counsel:

(a) Admits, accepts and acknowledges responsibility for illegal exports caused by its employees, partners, and subsidiaries acting on SAP's behalf, as set forth in the Statement of Facts in Attachment A, and agrees not to make any public statement contradicting those facts;

(b) Agrees that if it, or any of its current or future direct or indirect subsidiaries or affiliates, issues a press release or holds any press conference in connection with this Agreement, the Company shall first consult the Offices to determine: (a) whether the text of

the release or proposed statements at the press conference are true and accurate with respect to matters between the Offices and the Company; and (b) whether the Offices have any objection to the release. If the Offices determine that a public statement by any such person contradicts in whole or in part a statement contained in the Statement of Facts, the Offices shall so notify the Company, and the Company may avoid a breach of this Agreement by publicly repudiating such statement(s) within five business days after notification.

(c) Agrees that SAP's obligations under this agreement shall have a term of three years from the date on which the Agreement is executed (the "Agreement Term"). SAP agrees, however, that, in the event the Offices determine, in their sole discretion, that SAP has knowingly violated any provision of this Agreement or has failed to completely perform or fulfill each of their obligations under this Agreement, an extension or extensions of the Agreement Term may be imposed by the Offices, in their sole discretion, for up to a total additional time period of one year, without prejudice to the Offices' right to proceed as provided in the breach provisions of this Agreement below. Any extension of the Agreement extends all terms of this Agreement.

(d) Agrees to cooperate with the Offices, as described in paragraph 5 below;

(e) Agrees that during the Agreement Term, SAP will not commit any federal criminal offenses, and specifically will not knowingly violate the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701 *et seq.*, the Export Control Reform Act, 50 U.S.C. §§ 4801 *et seq.*, the Export Administration Regulations, 15 C.F.R. Part 730 *et seq.*, the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560, the Arms Export Control Act, 22 U.S.C. § 2778, or the International Traffic in Arms Regulations 22 C.F.R. parts 120-130 (collectively, "Export Offenses");

(f) Is committed to continuing to enhance its corporate compliance program, including ensuring that its compliance program satisfies the minimum elements set forth in Attachment B to this Agreement (Corporate Compliance Program) to the extent they are not already part of the Company's existing internal controls; and

(g) Agrees that annually during the Agreement Term, including between thirty and sixty days before the expiration of the Agreement Term, the Chief Export Controls Officer/Executive Board Member of SAP shall execute, under penalty of perjury, and provide to the Offices, a certification that, to the best of his or her knowledge after reasonable inquiry sufficient to assess compliance, SAP is in compliance with the terms of this Agreement. Each certification will be deemed a material statement and representation by the Company to the executive branch of the United States for purposes of 18 U.S.C. § 1001.

5. SAP shall cooperate fully with the Offices in any and all matters relating to the conduct described in this Agreement and the attached Statement of Facts and other conduct under investigation by the Offices at any time during the Agreement Term, until the later of the date the Agreement Term ends or the date upon which all investigations and prosecutions arising out of such conduct are concluded. At the request of the Offices, SAP shall also cooperate fully with

other domestic or foreign law enforcement and regulatory authorities and agencies in any investigation of SAP, its subsidiaries or affiliates, or any of its present or former officers, directors, employees, agents, and consultants, or any other party, in any and all matters relating to the conduct described in this Agreement and the attached Statement of Facts and other conduct under investigation by the Offices at any time during the Agreement Term. SAP's cooperation pursuant to this Paragraph is subject to applicable law and regulations, as well as valid claims of attorney-client privilege or attorney work product doctrine; however, SAP must provide to the Offices a log of any information or cooperation that is not provided based on an assertion of law, regulation, or privilege, and SAP bears the burden of establishing the validity of any such an assertion. SAP agrees that its cooperation shall include, but not be limited to, the following:

(a) Truthfully and in a timely manner disclosing all factual information with respect to their activities, those of their subsidiaries and affiliates, and those of their present and former directors, officers, employees, agents, and consultants, including any evidence or allegations and internal or external investigations, about which the Offices may inquire. This obligation of truthful disclosure includes, but is not limited to, the obligation of SAP to promptly provide to the Offices, upon request, any and all non-privileged documents, records, information, tangible evidence and other materials (with translations in English), wherever located, in the possession, custody, or control of SAP or its subsidiaries about which the Offices may inquire of SAP;

(b) Upon request, providing a detailed privilege log for those documents, records, information, tangible evidence or other materials requested but withheld under a claim of privilege;

(c) Upon request of the Offices, designating knowledgeable employees, agents or attorneys to provide to the Offices the information and materials described above on behalf of SAP. It is further understood that SAP must, at all times, provide complete, truthful, and accurate information;

(d) Using its best efforts to make available for interviews or testimony, as requested by the Offices, present or former officers, directors, employees, agents, and consultants of SAP. This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with domestic or foreign law enforcement and regulatory authorities. Cooperation shall include identification of witnesses who, to the knowledge of SAP, may have non-privileged material information regarding the matters under investigation;

(e) With respect to any information, testimony, documents, records, or other tangible evidence provided to the Offices pursuant to this Agreement, consenting to any and all disclosures, subject to applicable law and regulations, to other governmental authorities, including United States authorities and those of a foreign government, of such materials as the Offices in their sole discretion shall deem appropriate; and

(f) During the Agreement Term, should SAP learn of any evidence or credible allegation of a violation of U.S. federal law, SAP shall promptly report such evidence or credible allegation to the Offices.

6. With respect to SAP's ethics program and export compliance program, SAP will comply with the provisions set forth in Attachment B. In addition, SAP will provide to the Offices copies of Audit Reports described below:

(a) SAP will enter into Administrative Agreements with the Department of Commerce, Bureau of Industry and Security ("BIS") and the Department of the Treasury, Office of Foreign Assets Control ("OFAC") ("Administrative Agreements"). The Administrative Agreements, however, are not incorporated herein and the Offices are not hereby made a signatory or party to those agreements. Among other things, the BIS settlement agreement requires that, for a period of three years, SAP conduct internal audits of its compliance with U.S. export control laws and regulations ("Audit Reports").

(b) SAP agrees it will provide a complete copy of the Audit Reports to the Offices at the same time those reports are provided to BIS as required under its Settlement Agreement. SAP agrees that the Offices may disclose the Audit Reports to any other federal law enforcement or regulatory agency in furtherance of an investigation of any other matters discovered by, or brought to the attention of, the Offices. SAP may identify any trade secret or proprietary information contained in the Audit Reports and request the information be redacted prior to disclosure.

7. The Company agrees to pay a total monetary penalty in the amount of \$5,140,000 (the "Total Monetary Penalty"). The Total Monetary Penalty reflects the gross revenue earned by the Company as a result of the conduct described in the Statement of Facts. The Company will pay the Total Monetary Penalty to the United States Treasury within ten business days of the signing of this Agreement. The Company acknowledges that no tax deduction may be sought in connection with the payment of any part of the Total Monetary Penalty. The Company shall not seek or accept directly or indirectly reimbursement or indemnification from any source of the penalty or disgorgement amounts that the Company pays pursuant to this Agreement or any other agreement entered into with an enforcement authority or regulator concerning the facts set forth in the attached Statement of Facts.

#### **Offices' Promises and Obligations**

8. In exchange for SAP's good faith performance of its promises and obligations as set forth in this Non-Prosecution Agreement, the Offices agree not to seek any federal criminal charges against SAP or its subsidiaries relating to the conduct described in Attachment A. To the extent there is conduct disclosed by SAP that does not relate to any of the conduct described in the attached Statement of Facts, such conduct will not be exempt from prosecution and is not within the scope of or relevant to this Agreement. The Offices, however, may use any information related to the conduct described in the attached Statement of Facts against SAP: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a

prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code. This Agreement does not provide any protection against prosecution for any future conduct by SAP or any of their present or former parents or subsidiaries. In addition, this Agreement does not provide any protection against prosecution of any individuals, regardless of their affiliation with SAP or any of its present or former parents or subsidiaries.

### **Breach**

9. Should the Offices determine in good faith, and in their sole discretion, that SAP has failed to provide full and truthful cooperation, as described in paragraph 5 above, or has otherwise violated any provision of this Non-Prosecution Agreement, regardless of whether the Offices become aware of such a breach after the Term is complete, the Offices will notify counsel for SAP of their intention to void any of their obligations under this agreement (except their obligations under this paragraph), and SAP shall be subject to prosecution for any federal crime of which the Offices have knowledge, including but not limited to false statements, perjury, obstruction of justice and the Export Offenses described in Attachment A. SAP agrees, in the event of such breach of this Agreement, that the Offices may bring a prosecution within one year of their notification of breach of this Agreement of any criminal charge the statute of limitations for which had not expired as of the signing of this Agreement. Thus, by signing this Agreement, SAP agrees the statutes of limitation of all potential criminal charges related to the violations described in Attachment A have not expired on the date of this Agreement and would be deemed tolled, if this agreement is breached, until one year following the Offices' notification of said breach. In the event of such a breach, SAP agrees it waives any claim or defense based on the statute of limitations, any claim of pre-indictment delay, or any speedy trial claim with respect to any prosecution relating to the violations described in Attachment A, to the extent that such claims or defenses existed on the date SAP signed this Non-Prosecution Agreement.

10. In addition, the Company agrees that the statute of limitations as to any export control violation of U.S. federal law that occurs during the Agreement Term will be tolled from the date upon which the violation occurs until the earlier of the date upon which the Offices are made aware of the violation or the duration of the Agreement Term plus five years, and that this period shall be excluded from any calculation of time for purposes of the application of the statute of limitations. Provided, however, that nothing in this Agreement shall revive a statute of limitations that expired prior to the time that this Agreement was executed.

11. In the event the Offices determine that SAP has breached this Agreement, the Offices agree to provide SAP with written notice of such breach prior to instituting any prosecution resulting from such breach. Within thirty days of receipt of such notice, SAP shall have the opportunity to respond to the Offices in writing to explain the nature and circumstances of such breach, as well as the actions SAP has taken to address and remediate the situation, which explanation the Offices shall consider in determining whether to pursue prosecution of SAP or its subsidiaries or affiliates.

12. SAP understands and agrees that in any further prosecution of it resulting from a breach of this agreement, (A) any and all statements made by SAP, its subsidiaries, employees, and/or agents to the Offices or other designated law enforcement agents, whether prior to or after the signing of this agreement, including Attachment A hereto, and any testimony given by SAP, its subsidiaries, employees, and/or agents before a grand jury or other tribunal, whether prior to or after the signing of this agreement, and any leads from such statements or testimony, shall be admissible in evidence in any criminal proceedings brought against SAP, its subsidiaries, employees, and/or agents; and (B) SAP shall assert no claim under the United States Constitution, any statute, rule-based privilege, Rule 410 of the Federal Rules of Evidence, Rule 11(f) of the Federal Rules of Criminal Procedure, or any other federal rule that such statements or any leads therefrom should be suppressed. By signing this Non-Prosecution Agreement, SAP waives all rights in the foregoing respects.

#### **Miscellaneous Provisions**

13. SAP warrants and represents that its undersigned Chief Executive Officer is authorized to execute and deliver this Non-Prosecution Agreement and has the authority, granted by SAP's Supervisory Board, to bind SAP to its terms. The Offices warrant and represent that the undersigned representatives are authorized to execute and deliver this Agreement and bind the Offices to its terms.

14. SAP agrees that if it sells or merges all or substantially all of its business operations as they exist as of the date of this Non-Prosecution Agreement during the term of this Non-Prosecution Agreement, it shall include in any contract for sale or merger, a provision binding the purchaser/successor to the obligations described in this Non-Prosecution Agreement and this Agreement shall remain in effect.

15. This Agreement is binding on SAP and the Offices, but specifically does not bind any other component of the Department of Justice, other federal agencies, or any state, local or foreign law enforcement or regulatory agencies, or any other authorities, although the Offices will bring the cooperation of SAP and their compliance with their other obligations under this Agreement to the attention of such agencies and authorities if requested to do so by SAP.

16. All notices or reports to the Offices required or permitted by this Non-Prosecution Agreement shall be in writing and shall be sent by overnight mail, fax, or e-mail, and addressed as follows:

Department of Justice  
National Security Division  
Counterintelligence and Export Control Section  
Attn: Heather Schmidt  
950 Pennsylvania Ave. N.W.  
Room 7750  
Washington, D.C., 20530  
E-mail: [Heather.Schmidt@usdoj.gov](mailto:Heather.Schmidt@usdoj.gov); and

United States Attorney's Office  
for the District of Massachusetts  
Attn: Stephanie Siegmann  
John Joseph Moakley Courthouse  
1 Courthouse Way  
Suite 9200  
Boston, MA 02210  
E-mail: Stephanie.Siegmann@usdoj.gov.

17. This Non-Prosecution Agreement, Attachment A, and Attachment B hereto constitute the entire agreement. Except as set forth herein, there are no promises, understandings or agreements between the Offices and SAP or SAP's counsel. No additional agreement, understanding or condition may be entered into unless in a writing signed by duly authorized representatives of the Offices and SAP.

18. This Non-Prosecution Agreement is covered by the laws of the United States. The parties agree that exclusive jurisdiction and venue for any dispute arising under this Non-Prosecution Agreement is in the United States District Court for the District of Massachusetts.

19. It is further understood that SAP and the Offices may disclose this Non-Prosecution Agreement to the public.

20. This Non-Prosecution Agreement may be executed in counterparts, each of which constitutes an original and all of which constitute one and the same agreement. Fax or electronically submitted signatures are acceptable, binding signatures for purposes of this Non-Prosecution Agreement.

Sincerely,

Date:

April 29, 2021

  
Jay I. Bratt  
Chief

Counterintelligence and Export Control Section  
National Security Division  
Department of Justice

Date:

April 24, 2021


  
Nathaniel R. Mendell  
Acting United States Attorney  
District of Massachusetts



AGREED AND CONSENTED TO:

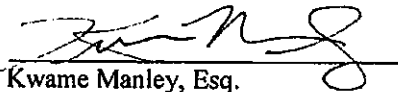
SAP:   
Christian Klein  
Chief Executive Officer  
SAP SE

Date: April 23, 2021

SAP:   
Luka Mucic  
Chief Financial Officer  
SAP SE

Date: April 21, 2021

REVIEWED AND APPROVED:

By:   
Kwame Manley, Esq.  
Robert Luskin, Esq.  
Paul Hastings LLP  
Attorneys for SAP SE

Date: April 23, 2021

## **ATTACHMENT A: STATEMENT OF FACTS**

1. The following Statement of Facts is incorporated by reference as part of the Non-Prosecution Agreement (the “Agreement”) between the National Security Division of the United States Department of Justice and the United States Attorney’s Office for the District of Massachusetts (collectively, “DOJ”) and the defendant, SAP SE (“SAP” or “the Company”). SAP hereby agrees and stipulates that the following information is true and accurate.

### **Relevant Entities**

2. SAP is a global software company headquartered in Walldorf, Germany. SAP provides a broad array of software licenses and maintenance support, cloud subscriptions, and professional services. With more than 425,000 customers in over 180 countries, SAP has a global presence and employs more than 96,000 people.

3. SAP controls a worldwide group of subsidiaries that develop, distribute, and provide SAP products and services. SAP subsidiaries relevant to the Agreement include SAP Ariba, Inc. (“Ariba”), based in Palo Alto, California; SAP Concur Technologies, Inc. (“Concur”), based in Bellevue, Washington; SAP SuccessFactors, Inc. (“SuccessFactors”), based in San Francisco, California; SAP Fieldglass (“Fieldglass”), based in Chicago, Illinois; SAP CallidusCloud (“CallidusCloud”), based in Dublin, California;<sup>1</sup> SAP Middle East North Africa (“SAP MENA”), based in Dubai, United Arab Emirates; SAP Türkiye Yazılım Üretim ve Ticaret A.Ş. (“SAP Turkey”), based in Istanbul, Turkey; and SAP Malaysia Sdn. Bhd. (“SAP Malaysia”), based in Kuala Lumpur, Malaysia.

---

<sup>1</sup> Ariba, Concur, SuccessFactors, Fieldglass, and CallidusCloud are collectively referred to as the “SAP Cloud Business Group” or “CBGs.”

4. In addition to selling products and services directly to customers, SAP has a broad network of independent third-party resellers, known as SAP Partners ("SAP Partners"). SAP Partners re-sell software licenses to customers worldwide, assist with maintenance and logistical support, and engage in other consulting activity regarding SAP products.

5. SAP customers access certain software, as well as upgrades and patches, by downloading them from online SAP portals. These downloads are delivered to customers either directly through an SAP server or indirectly through a server hosted by SAP's U.S.-headquartered Content Delivery Provider ("Content Delivery Provider"). SAP provides instruction to the Content Delivery Provider regarding which downloads to provide to which users.

6. Many SAP products contain U.S.-origin material and are subject to U.S. Export Administration Regulations ("EAR").

### **Relevant Law**

#### **International Emergency Economic Powers Act**

7. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1701 et seq., gave the President of the United States broad authority to regulate exports and other international transactions in times of national emergency. IEEPA controls are triggered by an Executive Order declaring a national emergency based on an "unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States." Pursuant to the authority under IEEPA, the President and the executive branch have issued orders and regulations governing and prohibiting certain practices and transactions with respect to various sanctioned nations by U.S. persons or involving U.S.-origin goods.

8. It is a crime for a person to willfully commit, willfully attempt to commit, willfully conspire to commit, or willfully cause a violation of any license, order, regulation, or prohibition issued under IEEPA, 50 U.S.C. § 1705.

### **Iranian Transactions and Sanctions Regulations**

9. On March 15 and May 6, 1995, the President issued Executive Orders Nos. 12957 and 12959, pursuant to IEEPA, prohibiting, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, to the Islamic Republic of Iran ("Iran") of any goods, technology, or services from the United States or by a United States person, and on August 19, 1997, issued Executive Order No. 13059 clarifying the previous orders (collectively, the "Executive Orders"). The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations (reissued and renamed in 2012 the Iranian Transactions and Sanctions Regulations, the "ITSR") implementing the sanctions imposed by these Executive Orders.

10. The ITSR, Title 31, Code of Federal Regulations, Part 560, prohibit, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, of any goods, technology, or services to Iran or the Government of Iran (with certain limited exceptions), including the exportation, reexportation, sale or supply of goods, technology, or services to a third country knowing or having reason to know that such goods, technology, or services are intended for Iran or the Government of Iran, without a license from OFAC. 31 C.F.R. § 560.204.

11. The ITSR further prohibit transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate the ITSR. 31 C.F.R. § 560.203.

12. Additionally, the reexportation from a third country, directly or indirectly, by a person other than a United States person, of any goods, technology, or services that have been exported from the United States is prohibited, if: (1) Undertaken with knowledge or reason to know that the reexportation is intended specifically for Iran or the Government of Iran; and (2) The exportation of such goods, technology, or services from the United States to Iran was subject to export license application requirements under any United States regulations in effect on May 6, 1995, or thereafter is made subject to such requirements imposed independently of this part (see § 560.414). 31 C.F.R. § 560.205.

---

### Overview

13. Starting in approximately January 2010, and continuing through approximately September 2017 (the “relevant time period”), SAP, without a license, willfully exported, re-exported, sold, or supplied, or caused the export, re-export, sale, or supply, of U.S.-origin technology or services to companies and individuals in Iran, in violation of IEEPA and the ITSR.

14. Specifically, SAP released thousands of downloads of SAP products, upgrades, and/or patches to Iranian users, including via its U.S.-headquartered Content Delivery Provider. The downloads occurred because: (i) certain SAP Partners willfully sold SAP on-premises software and related services to companies in Iran without the requisite license; and (ii) a number of multinational SAP customers, headquartered outside of Iran, engaged in the use of SAP products and services in Iran without a license.

15. SAP further permitted thousands of Iranian users to access SAP cloud services, which are maintained and supported in the U.S. and by U.S. employees worldwide.

16. On September 8, 2017, SAP made a voluntary self-disclosure to DOJ's National Security Division and the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") regarding potential violations of the ITSR. On January 11, 2018, SAP prepared an additional voluntary self-disclosure to the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") regarding potential violations of the EAR.

#### **SAP On-Premise Downloads to Iran**

17. During the relevant time period, SAP customers typically accessed the on-premise software they purchased, as well as upgrades and patches for that software, by downloading it from SAP.<sup>1</sup> These downloads were delivered to customers either directly through an SAP server or indirectly through a server hosted by SAP's Content Delivery Provider.

18. Between 2010 and 2017, SAP's U.S.-headquartered Content Delivery Provider released SAP software, upgrades, and/or patches 5,787 times to SAP users in Iran, allowing those users to access and download SAP technology. SAP's own servers released an additional 19,567 downloads to Iran. As described below, these 25,354 downloads went to 14 Iranian shell companies and several multinational companies.

#### **SAP Failed to Act on Identified Gaps in Export Control Processes**

19. SAP conducted several internal audits of its export controls processes over the years, including in 2006, 2007, 2010, and 2014. The 2006 audit highlighted that SAP was not identifying the country to which on-premise software and support products were being downloaded, and that SAP was accordingly at risk of breaching applicable U.S. export controls and sanctions. The 2006 audit recommended implementing tools to verify the location of the user

---

<sup>1</sup> For purposes of this agreement, "on-premise" refers to software installed and running on computers at the customer's location.

making the download requests.

20. Subsequent audits continued to identify gaps in the Company's export controls processes. For example, the 2014 audit report identified that SAP did not screen customers' IP addresses to prevent users with IP addresses in U.S.-embargoed countries from downloading SAP products. The 2014 audit similarly recommended that SAP implement geo-location IP address screening.

21. These audit reports were provided to senior SAP managers, including SAP Board members, the Legal Counsel in the United States responsible for export controls, and the Head of Logistics. Nonetheless, the Company did not implement geo-location controls until 2015, although it was aware of and had the ability to implement such controls before that time. As a result, SAP released thousands of downloads to end-users in Iran.

22. In July 2015, SAP implemented geo-location IP address blocking for its on-premise download delivery portal. It also requested its Content Delivery Provider to activate its geo-location IP address screening for all transactions, a function which the Content Delivery Provider had possessed for many years, but which the Content Delivery Provider had only been using intermittently. This screening ensures that users with a geo-location or IP address associated with a sanctioned jurisdiction are prevented from downloading SAP software via the Company's authorized on-premise software delivery channels.

#### **SAP Partner Sales to Iranian Shell Entities**

23. During the relevant time period, SAP Partners in Turkey, UAE, Germany, and Malaysia distributed SAP on-premise software to Iran via 14 foreign-registered front companies. These 14 front companies were, in fact, Iranian-controlled and served as pass-through entities,

which enabled 24,634 downloads of SAP products, updates, and/or patches for exclusive use in Iran.

24. SAP received various whistleblower complaints over the years, including as early as 2011, alleging sales by SAP Partners to foreign-registered affiliates of Iranian companies, but SAP failed to investigate those reports. It was not until late 2017 that SAP conducted on-site examinations of SAP Partners, and confirmed that certain SAP Partners sold SAP products to the Iranian front companies. These examinations included interviews with relevant employees; scrutiny of policies, procedures and internal controls; and analysis of financial and transactional data. The examinations revealed that certain SAP Partners had failed to conduct an adequate level of due diligence prior to making sales to the front companies. Moreover, however, certain SAP and SAP Partner executives, including senior leaders at SAP MENA, knew the front companies that purchased the SAP software had done so with the intent of using the Company's products in Iran in violation of U.S. law. In fact, publicly available information posted on certain SAP Partners' websites touted their business ties to Iranian companies, and posts on social networking websites highlighted the presence of SAP products in Iran.

#### **Multinational Customer Usage in Iran**

25. During the relevant time period, an additional 31 SAP customers made 720 total confirmed downloads of SAP products in Iran. All of the 720 downloads of SAP software, upgrades, and/or patches were delivered via SAP's U.S.-Headquartered Content Delivery Provider.

26. The 31 customers were primarily multinational companies, conducting legitimate operations in countries that were not subject to U.S. sanctions. SAP's controls, as well as those implemented by its Content Delivery Provider, failed to prevent the download activity in Iran.



### **SAP Cloud Business Group**

27. Since 2011, SAP has acquired various Cloud Business Group companies ("CBGs") in the United States.<sup>1</sup> Pre-acquisition due diligence conducted by SAP's external counsel identified that these cloud companies lacked comprehensive export control and sanctions compliance programs, policies and procedures. In addition, SAP conducted post-acquisition export control-specific audits, which further confirmed that these businesses were lacking adequate export control and sanctions compliance processes.

28. Notwithstanding these findings, SAP made the decision to allow these companies to continue to operate as standalone entities, without being fully integrated into SAP's more robust export controls and sanctions compliance program. As a result, SAP did not adequately address the compliance gaps until 2017, when SAP initiated this internal investigation.

29. Due to the lack of controls, including the failure to implement geo-location IP address blocking, SAP CBGs permitted users in Iran to access U.S.-based cloud services. In total, approximately 2,360 Iranian users accessed such services.

### **Gross Gain**

30. In total, the Company was paid \$5.14 million for the illegal downloads and CBG services.

---

<sup>1</sup> SAP acquired Ariba in 2012. Ariba provides cloud-based procurement and supply chain management solutions. SAP acquired SuccessFactors in 2011. SuccessFactors provides cloud-based human resource software solutions. SAP acquired Concur in 2014. Concur provides cloud-based travel and expense management software. SAP acquired Fieldglass in 2014. Fieldglass offers cloud-based vendor and external workforce management programs. SAP acquired CallidusCloud in 2018. CallidusCloud provides cloud-based sales performance and learning management software.

## **ATTACHMENT B**

### **CORPORATE COMPLIANCE PROGRAM**

In order to address any deficiencies in its compliance code, policies, and procedures regarding compliance with U.S. export controls and sanctions laws, including the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701 *et seq.*, the Export Control Reform Act, 50 U.S.C. §§ 4801 *et seq.*, the Export Administration Regulations, 15 C.F.R. Parts 730-774, the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560, the Arms Export Control Act, 22 U.S.C. § 2778, or the International Traffic in Arms Regulations 22 C.F.R. Parts 120-130 (collectively "Export Control and Sanctions Laws"), SAP (the "Company") agrees to continue to conduct, in a manner consistent with all of its obligations under this Agreement, appropriate reviews of its existing internal controls, policies, and procedures.

Where necessary and appropriate, the Company agrees to continue to maintain and enhance existing internal controls, compliance code, policies, and procedures in order to ensure that it maintains a rigorous export controls and sanctions compliance program that includes policies and procedures designed to detect and deter violations of the Export Control and Sanctions Laws. As an initial matter, SAP must consult OFAC's "Framework for OFAC Compliance Commitments," and ensure that it is adhering to the elements described in the framework, specifically, (1) Senior Management Commitment, (2) a Risk Assessment, (3) Internal Controls, (4) Testing and Auditing, and (5) Training. Additionally, SAP agrees to the following elements, to the extent they are not already part of the Company's existing export controls and sanctions compliance code, policies, and procedures. SAP shall:

(1) Implement an effective system for internal reporting of suspected or actual violations of any Export Control and Sanctions Laws; SAP's export compliance policies, controls or procedures; or SAP's ethics policy related to export compliance policies, controls, or procedures. To the extent and where legally permissible, SAP shall maintain a confidential, anonymous "hotline" and e-mail address, that directors, officers, employees, agents and business partners of SAP, and its subsidiaries, are informed of and can use to notify SAP of any suspected or actual violations of any U.S. export control or sanctions laws; SAP's export compliance policies, controls, or procedures; or of SAP's ethics policy related to such export compliance policies, controls, or procedures. All messages received on the hotline and e-mail shall be reviewed by SAP's Head of Export Controls and/or Group Chief Compliance Officer within five business days of receipt. SAP shall prominently post information about this hotline and e-mail address on its website and shall inform all those who avail themselves of the hotline and e-mail reporting system of SAP's commitment to non-retaliation and to maintaining the confidentiality and anonymity of such reports.

(2) Conduct mandatory annual corporate ethics and export control training of all directors, officers and, as appropriate for job function, employees of SAP and its subsidiaries. SAP shall track and record completion of such export training by its directors, officers, and employees. Export training shall cover, at a minimum, (A) all relevant U.S. export control and sanctions laws; (B) SAP's Code of Business Conduct; (C) SAP's export compliance policies, controls, and procedures, including recordkeeping requirements; and (D) the obligations assumed by, and

responses expected of, directors, officers, and employees of SAP and its subsidiaries, upon learning of any suspected or actual violations of any U.S. export control and sanctions laws, of SAP's export compliance policies, controls, or procedures, or of SAP's Code of Business Conduct related to such export compliance policies, controls, or procedures. SAP's Executive Board shall communicate to the training participants, in writing or by video, his or her review and endorsement of the export training and education programs. To the extent that it has not already done so, SAP shall commence providing this training within ninety (90) calendar days after the execution of this Non-Prosecution Agreement.

(3) To the extent that their respective business relationships with SAP and its subsidiaries can reasonably be expected to implicate export control issues and as appropriate for their respective jobs or business functions, inform agents, consultants, representatives, distributors, and partners of their obligation to comply with U.S. export control and sanctions laws and of their obligations to report any violations of U.S. export control and sanctions laws as they relate to SAP's products and services. To the extent that it has not already done so, SAP shall commence providing such individuals and entities with this information within one-hundred eighty (180) calendar days after the execution of this Non-Prosecution Agreement.

(4) Audit all newly acquired companies within 60 calendar days of acquisition to determine whether sufficient ethics and export enforcement controls are in place. If SAP identifies, during the pendency of this Non-Prosecution Agreement, any export violations during its audit, it agrees to identify the violations to the Offices within five (5) business days of the conclusion of the audit. If the newly acquired company does not have an export control system in place, or the existing export compliance program is not sufficient to prevent illegal exports, SAP will implement such a program within 90 calendar days of the conclusion of the audit. If additional time is necessary to implement an export compliance program, SAP will contact the Offices for an extension of time explaining the exigency.

(5) Promulgate an effective written system of discipline for all directors, officers, employees, agents, and business partners of SAP, and its subsidiaries, who are found to have violated any U.S. export control or sanctions laws; SAP's export compliance policies, controls or procedures; or SAP's ethics policy related to such export compliance policies, controls, or procedures.

(6) Consistent with the terms of the Non-Prosecution Agreement, provide prompt written notification by SAP to the Offices of any credible evidence of possible criminal conduct relating to any suspected or actual violations or attempted violations of any U.S. export control or sanctions laws by any officer, director, employee, agent, or business partner of SAP or its subsidiaries. At the request of the Offices, SAP shall provide the Offices with all relevant non-privileged documents and information concerning such allegations, including but not limited to internal audit reports, "whistleblower" complaints, civil complaints, and documents produced in civil litigation. In addition, to the extent SAP has an obligation to notify the Offices pursuant to this subsection, SAP shall report to the Offices its planned investigative measures and any resulting remedial measures, internal and external, as a result of any suspected or actual violations of any U.S. export control laws or regulations.