THIRD PARTY SECURITY AGREEMENT (“TPSA”)

DATED (“EFFECTIVE DATE”)

BETWEEN

(“SAP”)

AND

(“THIRD PARTY”)

THESE SAP THIRD PARTY SECURITY AGREEMENT are made as of (hereinafter the "**Effective Date**"), when signed by

with offices at

(“Third Party”)

on behalf of itself and its Third Party Affiliates become a binding agreement of Third Party towards SAP SE with offices at Dietmar-Hopp-Allee 16, 69190 Walldorf; Germany and SAP Affiliates; whereas "**SAP Affiliates**" shall mean any of SAP's affiliates and subsidiaries, meaning a corporation or other entity of which SAP owns, either directly or indirectly, more than fifty percent (50%) of the stock or other equity interests. (hereinafter "**SAP**").

THE THIRD PARTY HEREBY AGREES AS FOLLOWS:

This agreement is entered into between the parties identified above and effective as of the effective date. Whenever Third Party stores or processes any SAP Data (defined below), Third Party shall comply with the requirements of this TPSA and shall contractually require all of its sub-processors (including any subcontractor that is storing, using, or processing any SAP data in connection with Third Party’s delivery of services to SAP, including professional services and/or SaaS services (referred to herein as “Services”)) to comply with the requirements of this TPSA.

1. Definitions.

    a. “Third Party” means: an entity that has a business arrangement with SAP, by contract or otherwise, to provide products and/or services to, or on-behalf of, SAP and its subsidiaries; third parties may include suppliers of products and/or services or managed services.

    b. “SAP Data” means: any data, electronic or otherwise, to which Third Party has access in performing the Services, including, without limitation, any data specifically pertaining to SAP, its affiliates, or its employees, users, partners, customers, or suppliers.

    c. “System” means: a device or network of devices, virtual or actual, software, services and other elements connected together to store or process SAP Data, including, without limitation, Services.

    d. “Cardholder Data” means: (i) with respect to a payment card, the account holder’s name, account number, security codes, card validation code/value, service codes (*i.e.*, the three or four digit

number on the magnetic stripe that specifies acceptance requirements and limitations for a magnetic stripe read transaction), PIN or PIN block, valid to and from dates, and embedded data (including magnetic stripe data and EMV data); and (ii) information and data related to a payment card transaction that is identifiable with a specific account, regardless of whether or not a physical card is used in connection with such transaction.

e. "PCI Standards" means: the security standards for the protection of payment card information with which the payment card companies collectively or individually require merchants to comply including, but not limited to the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time, and any other applicable payment card industry data security requirements for Cardholder Data that are currently prescribed by the PCI Security Standards Council and as may be updated from time to time during the term of the TPSA.

f. "Vulnerability" means: a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.

g. "Non-Substantial Change" means: a clause(s) modification of phrasing or addition of clauses, which change the terminology without creating additional requirements or duties for the vendor outside of industry standards. This can include, but is not limited to, the creation of new actions to be taken by Third Party, but do not deviate from the spirit of current industry standard requirements.

h. "Substantial Change" means: a clause(s) modification which creates an additional Third Party requirement or duty that falls outside of current industry standard.

2. PCI Compliance. If Third Party has access to or will collect, access, use, store, process, dispose of or disclose Cardholder Data under this TPSA, Third Party shall at all times remain in compliance with the PCI Standards, including remaining aware at all times of changes to the PCI Standards and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI Standards, in each case, at Third Party's sole cost and expense.

3. Security Management. Third Party shall adopt, implement, maintain and monitor a written information security program that contains administrative, technical and physical safeguards designed to maintain service availability, data integrity, confidentiality and privacy of SAP Data, which program shall include:

   a. Executive review and support of all security related policies.
   b. Periodic (but no less than annual) risk assessments of all assets relevant to SAP.
   c. Periodic review of security incidents, including determination of root cause and corrective action.
   d. Periodic internal audit to measure the effectiveness of controls.

4. Security Standards. Without limiting Third Party's obligations herein, Third Party shall adhere to at least one of the following industry recognized security standards: ISO/IEC 27001 – Information Security Management Systems, or ISO-IEC 27002 – Code of Practice for International Security Management, the COBIT standards, NIST, or the PCI Standards.

5. Certifications/Attestations. Third Party is required to submit to SAP all current and applicable ISO/BS certifications (e.g., ISO27001 and ISO22301), System Organizational Control Reports (e.g., SOC2) or other certifications and attestations when available, and no more than annually, depending on the frequency of such audits, by using the electronic means as provided by SAP. SAP is entitled to share these certifications/attestations with SAP customers for whom the Third Party processes information or provides any type of indirect or direct maintenance or support.

6. Data Center Certifications/Attestations. Third Party must be certified against ISO 27001, PCI and provide SOC1 and SOC2 Type 2 reports as a minimum for all data center services. If data center services are subcontracted by the Third Party, the Third Party must ensure their subcontractors are also in compliance with these minimum requirements.

7. Penetration Testing. Third Party shall provide to SAP summary results of penetration testing undertaken by the Third Party of any Service processing SAP Data, upon request at Third Party's expense. Such testing shall occur no less frequently than once every twelve (12) months. If any such reports include any findings flagged as "critical," "high" or "medium" security risks (industry standards like Common Vulnerability Scoring System should be used for vulnerability rating), Third Party shall promptly fix such issues, undergo additional penetration testing, and provide a new report to SAP without any issues flagged as such level security risks. SAP is entitled to share these reports with SAP customers for whom the Third Party processes information or provides any type of indirect or direct maintenance or support.

8. Security Incident. Third Party shall notify SAP immediately (which in no event will be longer than twenty-four (24) hours) at https://www.sap.com/about/trust-center/security/incident-management.html whenever Third Party reasonably suspects that any SAP Data or Systems have been accessed, acquired, used or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose ("Incident"). Third Party acknowledges that this SAP point of contact address covers multiple affiliates, including SAP, and therefore agrees any such notices will contain a specific reference to "SAP Data." In parallel with providing such notice, Third Party shall without delay investigate the Incident, take necessary steps to eliminate or contain the exposures that led to such Incident, and keep SAP advised of the status of such Incident and all matters related thereto. Upon SAP's request, the Third Party must also provide an audit log of events that tracks service activity impacting SAP data upon SAP's request. Third Party further agrees to provide assistance, requested by SAP and/or SAP's designated representatives, in the furtherance of any investigation, correction and/or remediation of any such Incident, including any notification that SAP may determine appropriate to send to users, employees, customers or other individuals impacted or potentially impacted and/or the provision of credit monitoring service to such individuals, if and to the extent credit monitoring is required by applicable law. To the extent permitted by applicable laws or regulations, Third Party shall not give notice to any regulatory authority, any individual or any third party of any actual or potential Incident without first consulting with and obtaining SAP's written permission. SAP reserves the right to (i) immediately suspend the Services until it has determined that the Incident no longer poses a security or reputational risk to it, and (ii) immediately conduct additional on-site security audits and reviews of information concerning Third Party's security architecture, Systems and procedures. In the event of an Incident directly resulting from Third Party's failure to use industry standard security measures, including standard encryption protocols and the requirements set forth herein, Third Party shall be responsible for the cost of notification and, if applicable, credit monitoring as described above in this paragraph.

9. Human Resource Security. Third Party shall take reasonable steps to ensure the reliability of all Third Party employees and other Third Party personnel (together, "Personnel") who have access to SAP Data, including:

    a. Background Checks. Third Party shall require all Personnel who will have access to SAP Data to undergo and satisfy the requirements of a reasonable background investigation that Third Party conducts or causes to be conducted at its expense that is designed to confirm that none of such persons pose a threat to the safeguarding of SAP Data or other Confidential Information or a threat to the integrity of the business operations of SAP or any of its customers. In executing its pre-hire screenings, Third Party is responsible for conducting its background checks and decisions in accordance with applicable laws. At a minimum (and at all times in accordance with applicable

laws which may impose greater or different requirements), in order to be reasonable hereunder, background checks must include the following:

For personnel in the United States:

- SSN Trace
- 7 Year County Criminal Report
- 7 Year Statewide Criminal Report
- 7 Year Federal Criminal Report
- Basic Employment Verifications (all employment within 7 years)
- Education Verification (highest degree earned)
- Multi-state / Multi Jurisdiction Criminal Search
- Status on the Office of Foreign Assets Control (OFAC) list

For Personnel outside the United States:

- SSN or (or SSN equivalent) Trace (inapplicable if jurisdiction does not have an SSN equivalent)
- International Criminal Search (checking all locations listed on candidate profile)
- International Employment Verifications (checking all employment within past seven years)
- Education Verification (checking highest degree earned)

b. Security Policy and Confidentiality. Third Party shall require all Personnel to acknowledge in writing, at the time of hire and annually thereafter, to adhere to Third Party's security policy and to protect all SAP Data at all times, consistent with provisions of this Exhibit. Third Party will require all Personnel to sign a confidentiality statement with Third Party at the time of hire. Such policies shall be in accordance with on industry-accepted standards.

c. Security and Privacy Awareness Training. Third Party shall require all Personnel to undergo security and privacy awareness training, at the time of hire and annually thereafter.

d. Disciplinary Policy and Process. Third Party shall maintain a disciplinary policy and process, to be used when Personnel violate Third Party security or privacy policy or access SAP Data without prior authorization.

10. Access Management. Third Party shall use formal access management processes for the request, review, approval, and provisioning of all Third Party Personnel with access to any System. Access management controls will include:

a. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes.

b. Unique identifiers (user IDs) are required for access to all SAP data or systems. Procedures are in place so that requested user accounts and authorization changes are implemented only in accordance with approved policies and procedures that are based on industry best practices (for example, no rights are granted without authorization).

c. In case personnel leaves the company, their access rights are revoked within 24 hours. When personnel change their assigned role within the company, their access rights are timely revoked or adapted. Third Party has a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver

d. Display screens for all systems that could disclose information allowing access to another Third Party's device or system or screens used to handle confidential information should be positioned so that unauthorized persons cannot readily view them through a window, over a shoulder, or by similar means.

e. Mobile devices that could provide access to devices or systems where data is stored have to be kept in the possession of personnel or locked in a secure location when not in use. Mobile devices must not be checked in as luggage when travelling.

11. Malware Control. Third Party shall maintain effective malware controls, including:

    a. All Systems, all supporting Third Party systems, and all laptop computers, desktop computers, and mobile devices that access Systems will include commercial-grade anti-virus, anti-malware, anti-spyware controls that include real-time scanning, periodic whole-system scanning, and regular updates. This includes signature or behavior-based detections of malware, viruses, spyware and trojans as it applies to ingress and egress points such as email services and file transfers. It also mitigates security risks for malicious code on systems, endpoints, and devices.
    b. Third Party shall utilize spam-filtering systems to block incoming messages containing spam and malware.
    c. Third Party shall utilize web-filtering systems to block access to Internet web sites containing or suspected to contain malware.
    d. Third Party shall utilize commercial-grade firewalls that restrict all inbound and outbound traffic except for those specific ports and IP addresses necessary to perform the Service. Third Party continuously and actively detects systems and infrastructure against attacks through operation of an enterprise threat detection system and additional tools, including using and analyzing audit logs.

12. Intrusion Detection/ Intrusion Prevention. Third Party shall maintain network-based intrusion detection/ intrusion prevention system(s) to detect and prevent unwanted or hostile network traffic. Upon the availability of updates by the software provider, Third Party shall update its intrusion detection/prevention software promptly and without delay.

13. Data Encryption. Data cannot be read or modified without authorization during transfer and at rest. Third Party shall use current commercial industry standard secure encryption methods to protect SAP Data, including the following:

    a. Encryption of Transmitted Data. Third Party shall use current Internet-industry standard secure encryption methods designed to encrypt communications during transit between its server(s) / service(s) and SAP browser(s) and between all its servers and all SAP's server(s) / service(s) / end-points. This applies to both physical and network-based data transfer. Data in transfer within secured networks and networks in control of Third Party is appropriately secured.
    b. Encryption of Stored Data. Third Party shall use Internet-industry standard secure encryption methods to encrypt data at rest, including on mobile devices such as laptop computers, designed to protect stored SAP Data. Third Party shall store SAP Data only on server(s) that are segregated from servers accessed from the Internet by other users of Third Party services. Mobile devices that could provide access to devices or systems where data is stored use Third Party controlled network encryption when connecting to Third Party networks remotely.
    c. Encryption Key Management. Third Party shall have a defined key management policy that defines encryption key requirements, rotation, and lifecycle, including creation, distribution, revocation, archival, and destruction.

14. System Hardening. Third Party shall use Internet-industry standard system and device hardening standards for all Systems that store, process, or transmit SAP Data. Such hardening standards will include:

    a. Disable or remove all unnecessary services.
    b. Security patch management is implemented to provide regular and periodic deployment of relevant security updates.

c. Change all default passwords.
d. Rename administrative user accounts.
e. Each server performs only one function (e.g., web server, application server, and database server should occupy separate systems).
f. Employ host-based intrusion detection and prevention mechanism.
g. Passwords are stored using industry accepted hashing algorithm; only administrators that support the function have access to stored hashes, when necessary.

15. Incident Management. Third Party shall maintain (internal or external) incident management and forensics capabilities, policies and procedures, including detailed security incident escalation procedures.

16. Business Continuity. Third Party will ensure to monitor and document the reliability, maintainability, serviceability and availability of a system or service on a continuous basis. The Third Party shall conduct at least annual testing of the Third Party's Business Continuity Plan and provide a copy of the Business Continuity Plan and the results of the test to SAP upon request.

17. Stipulation of Availability. Third Party should ensure minimum availability of 99.99% per month, unless otherwise agreed upon in the relevant Statement of Work (SOW). Third Party will ensure Denial-of-Service (DoS) preventive measures are in place for the data center providing the service.

18. Vulnerability Management.

    a. Infrastructure Scans. Third Party shall perform periodic (but no less than once per month) vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities shall be remediated on a risk basis. Third Party shall install all Medium, High, and Critical security patches for all components in its production and development environment as soon as commercially possible.
    b. Application Scans. Third Party shall perform periodic (but no less than once per quarter, as well as after making any change to the Third Party System application vulnerability scans). Vulnerabilities shall be remediated on a risk basis. Third Party shall install all Medium, High, and Critical security patches for all components in its production and development environment as soon as commercially possible.
    c. External Application Testing. Third Party shall perform security code reviews, including both static testing and dynamic testing whenever changes occur to source code, or when new code is deployed.
    d. Vulnerability Notification. Third Party shall notify SAP of a confirmed Vulnerability without undue delay by sending notice of it to: vas@sap.com. The notice must include (I) a description of the Vulnerability, (II) impacted products or systems including the applicable versions, and (III) information reporting to the National Institute of Standards and Technology's Common Vulnerabilities and Exposures Program, including the CVE-ID, if applicable.

19. Data Management.

    a. Storage of Information. Third Party shall store SAP Data (to the extent permitted by the terms herein) only on servers controlled by Third Party and/or its third-party hosting provider. End user workstations, laptops, USB devices, CD-ROM, DVD-ROM, and mobile devices shall not be used to store any SAP Data.
    b. Segregation of Data. Third Party shall use physical and logical controls to segregate SAP Data from that of other customers. Third Party shall produce documentation describing data segregation controls to SAP upon request.

c. Backups. Third Party shall protect SAP data against loss, backup copies of information, software and system images shall be taken and tested regularly.

d. Change of the Hosting Provider. Third Party shall notify SAP at least 90 days in advance before changing or adding a hosting provider for Data or System deployment and such notice will identify the selected hosting provider (or provider options under consideration by Third Party). Third Party shall provide information as reasonably requested by SAP about the security practices and procedures of the selected provider, including its physical security controls and environment. In the event SAP reasonably determines that the security practices and physical security of the new provider are not sufficient or comparable to those employed by the hosting provider previously used by Third Party, SAP may terminate the Services with written notice of at least fifteen (15) days.

e. Change of Third Party (Fourth Party) Subcontractors. Third Party shall notify SAP at least 90 days in advance before changing subcontractors that will have access to SAP data or system that transmit, store, or process SAP data. Third Party shall provide to SAP on request any due diligence that was conducted to determine the subcontractor's suitability for performing services supporting SAP or SAP customers. SAP reserves the right of termination, both for Third Party's breach of security practice standards, or for violation of the 90 day limit.

f. Change of Third Party Processes. Third Party shall notify SAP of any major changes to processes the Third Party uses to support SAP or SAP customers at least 30 days in advance.

g. Return/Destruction of Data. As between SAP and Third Party, all SAP Data and data carriers and any copies, reproductions, summaries, analyses or extracts thereof or based thereon, including (without limitation) those made by Third Party in performance of the Services, are the property of SAP (including all customer and third party data SAP is responsible for) and shall be promptly returned via SAP approved methods to SAP upon any of the following events, whichever is earliest: (i) upon SAP's request; or (ii) upon completion of Services; or (iii) upon expiry or termination of any agreement under which Services are delivered. Alternatively, where SAP Data and/or data carriers cannot be returned, or if SAP elects so, Third Party shall destroy and certify to SAP in writing that it has permanently destroyed all SAP Data in its possession or control and data carriers which otherwise would have to be returned in accordance with this Section 16(d). The written certificate of destruction shall detail the destruction method used to permanently destroy all SAP Data and/or data carriers, the date of destruction and individual who performed the destruction. Third Party's destruction of SAP Data under this Section shall be in compliance with industry standard practices.

h. Third Party shall not access, use, store, transfer, or disclose any SAP Data, except as necessary to perform the Services.

20. Security Logs. Third Party shall employ procedures that all systems, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized logging system in order to enable the security audits referred to below. Additionally, Third Party shall employ the following procedures:

    a. Logs shall be retained for at least one (1) year.
    b. Logs shall not contain Confidential Information.
    c. Logs shall be protected from unauthorized modification or erasure.
    d. Logs shall be backed up on a daily basis.
    e. Logs shall be monitored for risk and functional anomalies.

21. Secure Remote Access. Third Party shall employ two-factor authentication for all remote access to internal and confidential information and systems.

22. Data Retention. Data will be securely retained for the time requirements and in the manner in accordance with privacy and regulatory laws for the region of demographic persons that the third party creates, stores, or processes. This may continue after the primary engagement or project is closed.

23. Issue Remediation Third Party agrees to work with SAP and their designees to remediate issues or risks identified through assessments, conducted on behalf of SAP or conducted on behalf of the Third Party. Third Party shall remediate at its cost those issues identified as high within 30 days, those identified as Medium or low within 90 days, provided that an issue is within the reasonable control of the Third Party.

24. Secure Development. The Third Party ensures that all software and services developed by the Third Party to provision the Third Party services, including those developed by the Third Party and those provided by others, have been developed following a secure software development lifecycle process which includes industry best practices for achieving and sustaining required security qualities for confidentiality, integrity and availability protection. In addition, software security vulnerabilities (see, for example the OWASP Top Ten or CWE listings) shall be avoided. The expected security measures and controls applied for software provisioning, such as Security Education of the development workforce, Secure Architecture and Design principles, Secure Coding practices, Security Testing methods and tools applied, Security Response to react timely on applicable software vulnerabilities that become known, as well as application security controls embedded and enforced by the software itself, such as identity management, authentication, authorization, encryption etc. shall be adequate to meet relevant business, technology and regulatory risks according to international standards such as ISO/IEC 27034. The Third Party has procedures in place to ensure integrity of software updates and can demonstrate that precautions are taken to ensure that any own or Third Party or open source software used for providing the Third Party services do not contain known backdoors, viruses, trojans or other kind of malicious code.

25. Security Audits by SAP. SAP is entitled to carry out security audits on the systems, security processes and procedures of the Third Party at least once per year and any time upon prior notification in the case of a request from an external authority, reasonable suspicion of a security incident or findings in documented security audits or other documentation provided to SAP. Should a security scan of Third Party's resources containing SAP/Customer information or personal data be required to identify or validate deficiencies, SAP shall identify the tools used for testing and the methods used. SAP and the Third Party shall mutually agree to the scope, approach and timing of such testing so that scanning does not interfere with Third Party's normal business operations and performance. Audit results shall contain only relevant information for the services provided to SAP. If security vulnerabilities are discovered during the check, the Third Party shall take reasonable steps to mitigate the security vulnerabilities and to minimize any damage from the security incident.

26. NDAA 889 Requirement. Compliance with the 2019 National Defense Authorization Act Section 889. If applicable, the Third Party does not utilize equipment or services provided by Huawei, ZTE, Hytera, Hikvision, or Dahua or their subsidiaries.

27. Regulatory and Legal requirements. Under the applicable regulations and laws, SAP and its customers are required to execute enhanced audit, disaster recovery (including backups) and other data protection requirements, current or in the future, whether directly or in support of customer's obligations. Accordingly, Third Party will:

    a. Allow regulator or customer on-site audit rights to the extent required by law.
    b. Provide responses to questionnaires to the extent specific responses are required by applicable regulations and laws.
    c. Allow for customer termination rights for any deficiencies or noncompliance with this agreement or any applicable regulation or laws that requires such right under the applicable circumstances.

28. SAP Third Party Risk Management (TPRM) Process. Third Party is required to undergo and complete the SAP TPRM process. In addition, Section “Issue Remediation” will apply for issue remediation. SAP reserves the right of service termination in both cases, if either the SAP TPRM Process or the issue remediation is not completed.

29. Legal Notice for Substantial and Non-Substantial Changes. SAP reserves the right to make periodic changes to the terms of the TPSA. SAP shall notify the Third Party of the changes. The SAP and the Third Party will agree in writing on Substantial Changes. The written form requirement can also be met by exchange of letters or with an electronically transmitted signature (e-mail transmission with scanned signatures, or other electronically permissible form of contract conclusion provided by or on behalf of SAP, such as the SAP DocuSign procedure). Jurisdictions which do not allow electronic signature may still meet physical mail requirement through DocuSign’s “print and sign” provision. The Third Party’s consent to Non-Substantial Changes is implicit by lack of objection. Any objections must be made in writing, either by digital or physical medium.

30. Governing Law and Venue. This TPSA shall be governed by German law and the venue for any disputes related to this TPSA shall be Karlsruhe, Germany.

IN WITNESS WHEREOF, the parties have so agreed as of the date written above.

_____	_____
Signature	Signature
_____	_____
Print name	Print name
_____	_____
Title	Title
_____	_____
Date	Date