Subunternehmer der DocuSign Inc.		
SupportSave Solutions, Inc.	United States	11132 Ventura Blvd, Suite 420, Studio City, CA 91604; Service location: Cebu City, Philippines

4. Technisch-organisatorische Maßnahmen der DocuSign

Die Technisch-organisatorischen Maßnahmen sind hinterlegt in Appendix 2 der EU Standardvertragsklauseln (siehe Anlage 3 „EU-Standardvertragsklauseln und ergänzende Klauseln“)

Dies sind:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. Personnel. Data importer's personnel will not process Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.
2. Data Privacy Contact. The data privacy officer of the data importer can be reached at the following address: DocuSign, Inc. Attn: Chief Privacy Officer 221 Main Street, Suite 1000, San Francisco, CA 94105
3. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data, as defined in the applicable service agreement/schedule for DocuSign Signature, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

DocuSign's Information Security Program is designed to protect the confidentiality, integrity, and availability of Customer Data processed through DocuSign Signature by using a multi-tiered technical, procedural, and people-related control approach in accordance with industry best practices and applicable laws and regulations. While DocuSign is responsible for its implementation and operation of the Information Security Program and the protection measures described herein, security and privacy with respect to cloud services such as DocuSign Signature are shared responsibilities between the parties. Customer acknowledges that it is responsible for using and enforcing the controls and functionality available within DocuSign Signature to support its own compliance requirements for the Processing of Customer Data in accordance with Customer's responsibilities to its end users and applicable laws and regulations.

1. **DEFINITIONS**. Unless otherwise defined in this EU CLAUSES, capitalized terms will have the meaning given to them in the Agreement.

"Personnel" means all employees and agents of DocuSign involved in the performance of DocuSign Signature service.

"Production Environment" means the System setting where software, hardware, data, processes, and programs are executed for their final and intended operations by end users of DocuSign Signature.

"Subcontractor" means a third party that DocuSign has engaged to performs DocuSign Signature service on behalf of DocuSign.

"Unsuccessful Intrusion(s)" means unsuccessful attempts at unauthorized access, use, disclosure, modification, or destruction Customer Data processed by DocuSign Signature. Examples include but are not limited to: broadcast

attacks on firewalls, denial of service attacks, port scans, login attempts, interception of encrypted data where the corresponding encryption key remains uncompromised.

2. APPLICABILITY. This Appendix 2 applies only to the processing of Customer Data through DocuSign Signature. Customer acknowledges that this Appendix 2 does not apply to any other DocuSign products or services that Customer may have now or in the future unless this Appendix 2 is specifically incorporated by reference in the Agreement for such products and services. To the extent Customer exchanges with DocuSign data or information that does not meet the definition of "Customer Data," such data or information will be treated in accordance with the confidentiality terms of the Agreement.
3. CUSTOMER RESPONSIBILITIES. DocuSign Signature provides Customer with certain features and functionalities that customer may elect to use, including the ability to retrieve and delete eDocuments in the System. Customer is responsible for properly (a) configuring DocuSign Signature, (b) using and enforcing controls available in connection with DocuSign Signature (including any security controls), and (c) taking such steps, in accordance with the functionality of DocuSign Signature, that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Customer Data, which include controlling the management of Authorized Users' access and credentials to DocuSign Signature, controlling Customer Data that is processed by DocuSign Signature; and controlling the archival or deletion of eDocuments in the System.
4. PERMITTED USE & DISCLOSURE. Subject to the requirements set forth in this Appendix 2, DocuSign will not process Customer Data in any manner other than as permitted or required by the Agreement or as otherwise instructed by Customer.
5. SECURITY MANAGEMENT.
   - 5.1 Information Security Program. DocuSign maintains a written information security program that includes policies, procedures, and controls governing the processing of Customer Data through DocuSign Signature in accordance with the terms of the Agreement and this Appendix 2 (the "Information Security Program"). DocuSign will maintain its Information Security Program in accordance with the ISO 27001 standard or such other alternative standards that are substantially equivalent to ISO 27001 for the establishment, implementation, and control of the Information Security Program. Additionally, DocuSign will maintain controls sufficient to meet the objectives of PCI DSS, SOC1 and SOC 2, or equivalent standards and will be assessed against those standards annually. Upon Customer's request, not to exceed once annually, DocuSign will provide Customer with third party attestations, certifications, and reports relevant to the establishment, implementation, and control of the Information Security Program, including DocuSign's ISO 27001 certification, PCI DSS Attestation of Compliance, Service Organization Controls (SOC) reports, or equivalent certifications and reports.
   - 5.2 Background Checks and Training. DocuSign conducts reasonable and appropriate background investigations on all Personnel in accordance with applicable laws and regulations. Personnel must pass DocuSign's background checks prior to being assigned to positions in which they will, or DocuSign reasonably expects them to, have access to Customer Data. DocuSign conducts annual mandatory security awareness training to inform its Personnel on relevant security procedures and the consequences of violating those procedures.
   - 5.3. Subcontractors. All Subcontractors: (a) are evaluated by DocuSign to ensure that such Subcontractors maintain appropriate physical, technical, organizational, and administrative controls consistent with the requirements of this Appendix 2; and (b) fall into scope for independent audit assessment as part of DocuSign's ISO 27001, or equivalent, audit, where their roles and activities are reviewed per control requirements. DocuSign remains responsible for the acts and omissions of its Subcontractors as if it had performed the acts or omissions itself and any subcontracting will not in any way reduce DocuSign's obligations to Customer under the Agreement.
   - 5.4. Risk and Security Assurance Framework Contact. Customer's account management team at DocuSign will be Customer's first point of contact for information and support regarding DocuSign's Information Security Program and obligations under this Appendix 2. The account management team will work directly with Customer to escalate Customer's questions, issues, and requests to internal DocuSign groups as necessary.
6. PHYSICAL SECURITY MEASURES. DocuSign maintains appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that process Cus-

tomer Data. DocuSign utilizes commercial grade security software and hardware to protect DocuSign Signature and the Production Environment.

6.1 Facility Access. Access to DocuSign's corporate facilities is tightly controlled. Visitors must sign in, agree to confidentiality obligations, and be escorted by Personnel at all times. The DocuSign security team reviews visitor logs on a regular basis. At termination of employment, DocuSign promptly revokes terminated Personnel's physical access to DocuSign all corporate facilities.

6.2 Data Center Access. DocuSign's commercial-grade data center service providers used in the provision of DocuSign Signature are included in DocuSign's ISO 27001 or equivalent certification and must maintain an on-site security operation responsible for all physical data center security functions and formal physical access procedures in accordance with SOC1 and SOC 2, or equivalent, standards.

7. LOGICAL SECURITY.

7.1. Access Controls. DocuSign maintains a formal access control policy and employs a centralized access management system to control employee access to the Production Environment.

(a) All access to the Production Environment is subject to successful two-factor authentication globally from both corporate and remote locations and is restricted to authorized Personnel who demonstrate a legitimate business need for such access. DocuSign maintains an associated access control process for reviewing and implementing access requests. DocuSign regularly reviews the access rights of authorized Personnel and, upon change in scope of employment necessitating removal or employment termination, Personnel access rights are removed.

(b) DocuSign monitors and assesses the efficacy of access restrictions applicable to the control of DocuSign's system administrators in the Production Environment by, for example, generating system individual administrator activity information and retaining such information for a period of at least 12 months.

7.2. Network Security. DocuSign maintains a defense-in-depth approach to hardening the Production Environment against exposure and attack. The Production Environment is isolated and includes commercial grade network management controls such as load balancers, firewalls, intrusion detection systems distributed across production networks, and malware protections. DocuSign compliments its Production Environment architecture with prevention and detection technologies that monitor all activity-generated, risk-based alerts to the relevant security groups.

7.3. Malicious Code Protection. DocuSign's information systems and file transfer operations have effective and operational anti-virus software. All anti-virus software is configured for deployment and automatic update. Anti-virus software is integrated with processes and will automatically generate alerts to DocuSign's Cyber Incident Response Team if potentially harmful code is dedicated for their investigation and analysis.

7.4. Code Reviews. DocuSign maintains a formal software development lifecycle that includes secure coding practices against OWASP and related standards. DocuSign performs both manual and automated code reviews. Engineering, product development, and product operations management review changes included in production releases to verify that developers performed automated and manual code reviews designed to minimize associated risks. In the event that a significant issue is identified in a code review, it is brought to senior management's attention and is closely monitored until resolution prior to release into the Production Environment.

7.5. Vulnerability Scans and Penetration Tests. DocuSign performs both internal and external vulnerability scanning and application scanning. Quarterly external scans and annual penetration tests against DocuSign Signature and the Production Environment are conducted by external qualified, credentialed, and industry recognized organizations. DocuSign will remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner and timeframe based on severity. DocuSign will provide third party attestations resulting from such vulnerability scans per independent external audit reports upon Customer's reasonable written request. Under no circumstance will Customer be permitted to conduct any vulnerability scanning or penetration testing against the Production Environment.

8. STORAGE, ENCRYPTION, AND DISPOSAL.
   8.1. Separation. DocuSign logically separates Customer Data located in its multi-tenanted Production Environment from other customer data.
   8.2. Encryption Technologies. DocuSign encrypts Customer Data in accordance with industry best practice standards. All access and transfer of data to and from DocuSign Signature is via HTTPS and DocuSign only supports industry recognized and best practice cipher suites. All eDocuments persisted on the Production Environment are encrypted with an AES 256-bit, or equivalent, encryption key.
   8.3. Disposal. DocuSign maintains a data disposal and re-use policy for managing assets and implements processes and procedures for equipment management and secure media disposal.
9. BUSINESS CONTINUITY AND DISASTER RECOVERY.
   9.1. Continuity Plan. DocuSign maintains a written business continuity and disaster recovery plan addressing the availability of DocuSign Signature ("Continuity Plan"). The Continuity Plan includes elements such as: (a) crisis management, plan and team activation, event and communication process documentation; (b) business recovery, alternative site locations, and call tree testing; and (c) infrastructure, technology, system(s) details, recovery activities, and identification of the Personnel and teams required for such recovery. DocuSign conducts a test of the Continuity Plan on an annual basis.
   9.2. DocuSign Signature Continuity. DocuSign's production architecture for DocuSign Signature is designed to perform secure replication in near real-time to multiple active systems in geographically distributed and physically secure data centers located in the United States of America and European Union. Infrastructure systems for DocuSign Signature have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Each data center supporting DocuSign Signature includes full redundancy and fault tolerance infrastructure for electrical, cooling, and network systems. The Production Environment servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability.
10. INCIDENT RESPONSE AND BREACH NOTIFICATION.
   10.1. General. DocuSign maintains tested incident response program managed and run by DocuSign dedicated Global Incident Response Team. The incident response team operates to a mature framework, which includes incident management and breach notification policies and associated processes. DocuSign's incident response program includes: initial detection; initial tactical response; initial briefing; incident briefing; refined response; communication and message; formal containment; formal incident report; and post mortem/trend analysis.
   10.2. Breach Notification. Unless notification is delayed by applicable law or the demands of law enforcement, DocuSign will promptly report to Customer the deliberate unauthorized acquisition, access, use, disclosure or destruction of Customer Data (a "Data Breach") following determination by DocuSign that a definite Data Breach has occurred. Any such report will be made to Customer and sent to the appropriate party at the address and contact information set forth on the Order Form or as otherwise provided by Customer. DocuSign's obligation to report a Data Breach under this Section is not and will not be construed as an acknowledgement by DocuSign of any fault or liability of DocuSign with respect to such breach. The obligations in this Subsection (Breach Notification) will not apply to Unsuccessful Intrusions.
   10.3. Breach Response Procedures.
      (a) DocuSign will promptly take reasonable measures to mitigate the cause of any Data Breach and to prevent future Data Breaches of similar nature. As information regarding a Data Breach is collected or otherwise becomes available to DocuSign, DocuSign will provide additional detail regarding the nature and consequences of the Data Breach and the corrective and remedial actions being taken.
      (b) Due to the encryption configuration and security controls associated with DocuSign Signature, DocuSign will not have access to or know the nature of the information contained within Customer's eDocuments and, as such, the parties acknowledge that it may not be possible for DocuSign to provide Customer with a description of the type of information or the identity of individuals that may be affected by a Data Breach. In the event of a Data Breach, Customer will be solely responsible for: (i) determining whether to

notify impacted individuals or entities; (ii) providing any notice deemed necessary by Customer; and (iii) for determining if regulatory bodies or law enforcement applicable to Customer or Customer Data need to be notified.

11. CUSTOMER AUDIT RIGHTS.

11.1. Regulatory Audit. If an on-site audit of DocuSign is required by Customer's governmental regulators, as supported by evidence and a written statement by Customer, Customer may, either itself or through a third party independent contractor selected by Customer and at Customer's sole expense, conduct an on-site audit of DocuSign's Information Security Program, including DocuSign's data centers and corporate facilities relevant to the security of Customer Data ("Regulatory Audit"). Unless a different notice or frequency is required by Customer's governmental regulators, a Regulatory Audit may be conducted by Customer once per year with at least sixty (60) days' advance written notice to DocuSign. If a Regulatory Audit requires the equivalent of more than two (2) business days of DocuSign Personnel's time to support such audit, DocuSign may charge Customer an audit fee at DocuSign's then-current rates for each day thereafter.

11.2. Audit for Breach. Following any Data Breach of Customer Data, DocuSign will, upon Customer's written request, promptly engage a third party independent auditor, selected by DocuSign and at DocuSign's expense, to conduct an on-site audit of DocuSign's Information Security Program, including DocuSign's data centers and corporate facilities relevant to the security of Customer Data. DocuSign will promptly provide Customer with the report of such audit.

11.3. Conditions of Audit.

(a) Audits conducted by Customer pursuant to this Section (Customer Audit Rights) must: (i) be conducted during reasonable times; (ii) be of reasonable duration; (iii) not unreasonably interfere with DocuSign's day-to-day operations; (iv) be conducted upon mutually agreed upon terms; and (v) made in accordance with DocuSign's security policies and procedures. DocuSign reserves the right to limit an audit of any of the following: configuration settings, sensors, monitors, network devices and equipment, files, or any other items that DocuSign reasonably determines may compromise the security of DocuSign Signature or the data of other DocuSign customers. For clarification, Customer's audit rights under this Section (Customer Audit Rights) do not include penetration testing or active vulnerability assessments of the Production Environment or DocuSign Systems within their scope.

(b) In the event that Customer conducts an audit through a third party independent contractor, such independent contractor must enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect DocuSign's confidential and proprietary information.

(c) Customer must promptly provide DocuSign with any audit, security assessment, compliance assessment reports and associated findings prepared by it or its third party contractors for comment and input prior to formalization and/or sharing with another third party.

Remediation and Response. If any audit performed pursuant to this Section (Customer Audit Rights) reveals or identifies any non-compliance by DocuSign of its obligations under the Agreement and this Appendix 2, then (a) DocuSign will work to promptly correct such issues; and (b) Customer may request feedback and information regarding corrective and remedial actions taken in relation to such audit for no more than 60 days after the date upon which such audit was conducted.