THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

MICROSOFT'S SUPPLIER SECURITY AND PRIVACY ASSURANCE PROGRAM DATA PROTECTION REQUIREMENTS INDEPENDENT VERIFICATION, VERSION 10

January 22, 2025

Prepared By:

RSM US LLP
300 South Tryon Street, Suite 1500
Charlotte, North Carolina 28202
www.rsmus.com

Amy Feldman
+1 216 927 8236
amy.feldman@rsmus.com

Submitted To:

KYG Trade, Inc.
220 Newport Center Drive, Suite 11391
Newport Beach, California 92660
www.kygtrade.com

Todd Smith
+ 1 949 803 0338
todd@kyg.ai

TABLE OF CONTENTS

EXECUTIVE SUMMARY

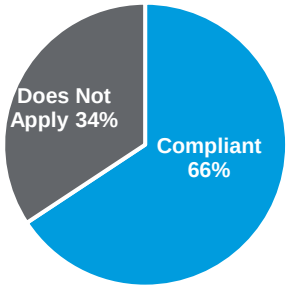
Purpose

The purpose of this engagement was to assess the design and operating effectiveness of the controls of KYG Trade, Inc. (or KYG) over Microsoft personal data and/or confidential data as defined in and in connection with the applicable sections and requirements of the Microsoft Supplier Data Protection Requirements (DPR) Version 10 as of January 17, 2025.

Because of inherent limitations, controls may not prevent, detect or correct errors or fraud that may occur. Also, projections of any evaluation of adequate design to future periods are subject to the risk that those controls may become inadequate because of change in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

Observations

While performing our verification, we identified that the organization was compliant in 46 of the 70 requirements assessed. The remaining 24 requirements were not in-scope.



Restricted Use

This letter is intended solely for the information and use of the supplier and Microsoft and is not intended to be and should not be used by anyone other than these specified parties.

We appreciate the courtesies and cooperation extended to us during this project and the opportunity to be of service to KYG Trade Inc. Please contact Amy Feldman at +1 216 927 8236 if you have any questions regarding this report.

Sincerely,

RSM US LLP

January 22, 2025

SSPA FINDINGS

Scope of the Assessment

The assessment was limited to the specific procedures described and was based on the information provided by the Supplier. Accordingly, information that was not made available or changes in circumstances after January 17, 2025, may affect the assessment results outlined below.

Assessment Procedures

To perform the verification, we reviewed the organization's inquiries with supplier contacts to develop an understanding of the design and operating effectiveness of the controls over applicable sections of Microsoft's DPR Version 10. While reviewing the DPR, we performed the following actions:

- We reviewed the supplier's inquiries with the supplier contact(s) to obtain an understanding of the design and operating effectiveness of the supplier's controls over the applicable sections of the DPR.
- We made observations of the supplier's policies and procedures to assess the evidence of compliance.
- We performed inspections of supplier's controls to assess the evidence of compliance over the applicable sections of the DPR.

Supplier and Assessment Information	
Supplier Name	KYG Trade, Inc.
Supplier Account Number(s)	0003061981
Supplier Address(es)	220 Newport Center Drive, Suite 11391 Newport Beach, California 92660
Assessor Contact(s)	Amy Feldman, RSM US LLP
Assessor Certification(s)	Certified Information Systems Security Professional (CISSP) Project Management Professional (PMP) Certified Third Party Risk Assessor (CTPRA)

Assessment Summary

While performing the verification, we did not identify any security gaps. While no security gaps were identified, we did not identify any mismatch responses, wherein the supplier claimed compliance to a specific requirement, but ultimately the requirement was not an applicable requirement. These are further detailed in the table provided in the detailed findings section of this report.

Results Overview	
No Gaps Found	No gaps were identified.
Response Mismatches (Claimed Compliance—Does Not Apply)	No responses were identified as mismatches.
Response Mismatches (Claimed Does Not Apply—Compliant)	No responses were identified as mismatches.

Assessment Results

Provided in the table below are the detailed results of the verification performed. This includes a detailed description of the procedure performed, the supplier response, our verification determination, and any additional remarks from the assessor.

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
Section A: Management				
1	We inspected “Request_1_EL-Microsoft Pilot.pdf” and “Evidence for Contract related language items.pdf.” We noted that a pilot agreement was maintained and effective. An updated agreement was pending upon completion of SSPA certification.	Compliant	Compliant	
3	Per inspection of “Head of DevOps - KYG Trade.pdf” and confirmation with KYG, Aslam Latheef (global head of IT and chief information security officer) had the responsibility and accountability for DPR compliance.	Compliant	Compliant	
4	We inspected the following: • “Security Awareness Training Policy.docx” • “Request_4_Evidence of Security Awareness Training.docx” • “Request_45b_initial_completion_Engineering_6-6-2024.xlsx” Per inspection, security and privacy training sessions were required to be completed annually and upon hiring.	Compliant	Compliant	
5	We inspected the following: • “Information Security Policy - v1.pdf” • “IT Security Policy.docx” • “Acceptable Use Policy - v1.pdf” • “Code of Conduct - v1 - unapproved.pdf” Per inspection, we noted that violations of these policies might result in disciplinary action, up to and including termination of employment or legal action.	Compliant	Compliant	
Section B: Notice				
Section C: Choice and Consent				
Section D: Collection				

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
Section E: Retention				
14	We inspected the following: • "Data Retention Policy Procedure.docx" • "Data Protection Policy.pdf" • "Data Classification Policy - v1 - unapproved.pdf" • "IT Security Policy.docx" Per inspection, we noted that data would be retained no longer than necessary to perform based on business, legal and contractual obligations.	Compliant	Compliant	
15	We inspected the following: • "Data Destruction policies and procedures.docx" • "Data Retention Policy Procedure.docx" • "Data Protection Policy.pdf" • "Data Retention Policy.docx" Per inspection, KYG had defined and implemented policies and procedures for the secure disposal of physical and digital data that was no longer necessary.	Compliant	Compliant	
Section F: Data Subjects				
Section G: Subcontractors				
25	Per confirmation, KYG acknowledged and agreed to notify Microsoft and obtain Microsoft's approval prior to subcontracting services or making any changes concerning the addition or replacement of subcontractors.	Compliant	Compliant	
26	Per KYG, Sayari provided forced labor risk screening, import/export risk models and supply chain mapping services.	Compliant	Compliant	
28	Per inspection of "Vendor Management Policy - v1 - unapproved.pdf" and confirmation with KYG, any data provided to a subcontractor was limited and only needed to perform contractual agreements.	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
30	We inspected the following: • "Vendor Management Policy - v1 - unapproved.pdf" • "KYG Trade Subcontractor Notice of Misuse clause.docx" • "Request_25_NDA-KYG Trade and ConceptVines 043023.pdf" Per inspection and confirmation with KYG, we noted that KYG had a process in place for subcontractors to report the misuse of data. KYG confirmed that there had been no reports of subcontractors misusing Microsoft data within the last 12 months.	Compliant	Compliant	
32	We inspected the following: • "Incident Response policies, procedures, and plan.docx" • "Incident Response Plan - v1 - unapproved.pdf" • "KYG Trade Subcontractor Notice of Misuse clause.docx" Per inspection, KYG had documented incident response policies and procedures to identify and handle any potentially harmful incidents of unauthorized use of data.	Compliant	Compliant	
Section H: Quality				
Section I: Monitoring and Enforcement				
34	We inspected the following: • "Incident Response policies, procedures, and plan.docx" • "Incident Response Plan - v1 - unapproved.pdf" Per inspection, KYG had an incident response plan in place to identify and handle incidents, including communicating the incident information to customers.	Compliant	Compliant	
35	We inspected the following: • "Incident Response policies, procedures, and plan.docx" • "Incident Response Plan - v1 - unapproved.pdf" Per inspection, KYG had an incident response procedure in place for responding to and handling incidents from initiation to closure.	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
Section J: Security				
37	We inspected the following: • "Request_36A_SRA - TE JCApp Status Update - 09-29-23.pptx" • "KYG Patch Management Policy.docx" • "Vulnerability Management Policy.pdf" Per inspection, KYG performed periodic vulnerability scans using a combination of external open-source and commercial tools. Penetration testing was performed by a certified penetration tester periodically.	Compliant	Compliant	
38	We inspected the following: • "Mobile Device Policy and Procedures.docx" • "Asset Management Policy - v1.pdf" • "Acceptable Use Policy - v1.pdf" Per inspection, KYG had defined and maintained a mobile device policy that secured mobile devices that accessed company and network resources.	Compliant	Compliant	
39	We inspected the following: • "Asset Management Policy - v1.pdf" • "Request_38 _Inventory_Azureresources.csv" Per inspection, KYG had an inventory of assets and an asset inventory process that was in place to classify and manage information assets.	Compliant	Compliant	
40	We inspected the following: • "System Access Control Policy - v1 - unapproved.pdf" • "Password Policy.pdf" • "Identification and Authentication Policy.docx" • "Data policies and procedures.docx" Per inspection, KYG had documented and maintained access rights management procedures to prevent unauthorized access.	Compliant	Compliant	
41	We inspected the following: • "KYG Patch Management Policy.docx" • "Vulnerability Management Policy.pdf" • Network Security Policy	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
	Per inspection, KYG had patch management procedures in place.			
42	We inspected the following: • "Vulnerability Management Policy.pdf" • "Asset Management Policy - v1.pdf" • "Acceptable Use Policy - v1.pdf" • "corey.png" • "defender.png" • "delsean.png" • "ev2-av.png" • "olga av.png" • "olga defender.png" • "screenshot (93).png" • "todd defender.png" Per inspection, KYG had virus and malware protection procedures and anti-virus tools were installed and up to date.	Compliant	Compliant	
43	We inspected the following: • "Secure Development Policy.docx" • "SoftwareDevelopmentLifeCyclePolicy.pdf" • "SDLC policies and procedures.docx Per inspection, KYG incorporated security-by-design principles in the build process of software and/or applications.	Compliant	Compliant	
44	We inspected the following: • "Network Security Policy - v1 - unapproved.pdf" • "Data Protection Policy.pdf" • "Logging and Monitoring Policy - v1 - unapproved.pdf" • "Data Backup Policy.docx" • "Evidence of DLP Using Microsft Purview.docx" Per inspection, KYG had a data protection program in place through established processes and procedures to prevent and detect suspicious or anomalous behavior and loss of data. Additionally, KYG used Microsoft Purview for data security purposes, including data loss prevention (DLP).	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
45	We inspected the following: • "SoftwareDevelopmentLifeCyclePolicy.pdf" • "SDLC policies and procedures.docx • "Secure Development Policy.docx" • "Evidence of no Hard Coded Secrets Snyk Code security rules _ Snyk User Docs.pdf" Per inspection, secret keys are not embedded or hard-coded in the software at any stage of the deployment process.	Compliant	Compliant	
46	We inspected the following: • "Backup Policy.docx" • "Data Backup Policy.docx" • "Data back up Policy Procedure.docx" • "Data Backup and Restoration Policy.docx" Per inspection, KYG had backup processes in place to periodically back up, securely store and effectively recover critical data.	Compliant	Compliant	
47	We inspected the following: • "BCP.docx" • "Disaster Recovery Plan - v1 - unapproved.pdf" • "kyg.ai - Disaster Recovery Restoration Test (AWS) .docx" • "kyg.ai - Disaster Recovery Restoration Test [Azure].docx" • "Disaster Recovery Restoration Test (AWS).docx" • "Disaster Recovery Restoration Test [Azure].docx" Per inspection, KYG had documented business continuity and disaster recovery plans in place, and procedures for responding to and recovering from disaster events were established, maintained and tested. The next business continuity plan testing will be completed in January 2025.	Compliant	Compliant	
48	We inspected the following: • "System Access Control Policy - v1 - unapproved.pdf" • "Password Policy.pdf" • "Identification and Authentication Policy.docx"	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
	• "Evidence of Notification to implement MFA.pdf" Per inspection, KYG's identification and authentication processes were place, including multifactor authentication and principle of least privilege.			
49	We inspected the following: • "Screenshot 2024-06-08 at 11.48.04 AM.png" • "Encryption Policy - v1 - unapproved.pdf" Per inspection, as part of KYG's session management, all user sessions were encrypted and secure protocols, such as Transport Layer Security (TLS), were used.	Compliant	Compliant	
50	We inspected the following: • "Data Classification Policy - v1 - unapproved.pdf" • "Data policies and procedures.docx" • "Encryption Policy - v1 - unapproved.pdf" • "bitlocker_screenshot.png" • "corey encry.png" • "olga.png" • "Screenshot (94).png" • "todd encryption.png" • "sukruth.png" Per inspection, KYG used BitLocker and FileVault to employ disk-based encryption.	Compliant	Compliant	
51	We inspected the following: • "Data Classification Policy - v1 - unapproved.pdf" • "Data policies and procedures.docx" • "Encryption Policy - v1 - unapproved.pdf" • "Request 51a_Storage account encryption.png" • "Request 51b_Screenshot 2024-06-07 at 1.22.27 AM.png" • "ev3.png" • "ev4.png" • "sukruth.png" • "jeff.png" Per inspection, data was encrypted at rest.	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
Section K: Artificial Intelligence (AI) Systems				
53	We inspected the following: • "KYG_AI_Addendum_v1 (1).docx" • "Request_1_EL-Microsoft Pilot.pdf" • "Evidence for Contract related language items.pdf" Per inspection, the addendum had required contractual terms on AI systems. Per confirmation with KYG, the AI addendum was communicated to Microsoft and was included in the final agreement.	Compliant	Compliant	
54	We inspected the following: • "KYG_AI_Policy_v2.docx" • "AI Org Chart - Deployment and Risk Management Accountability Structure.docx" Per inspection, chief artificial intelligence officer was responsible and accountable for AI management and compliance.	Compliant	Compliant	
55	We inspected the following: • "MSSSPA Q54 Evidence.docx" • "generative-ai_completion 12-17-2024.xlsx" • Screenshots of the generative AI learning objectives and completion rate Per inspection, KYG required completion of privacy and security training on generative AI for its employees upon hire and annually.	Compliant	Compliant	
56	We inspected the following: • "AI Incident Response Plan.docx" • "KYG_AI_Policy_v2.docx" Per inspection, KYG had a documented AI incident response plan in place for identifying, handling and notifying customers about incidents related to AI systems. KYG confirmed that there had been no incidents related to AI systems within the last 12 months.	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
57	Per inspection of the following, we noted KYG periodically conducted red team exercises within the AI environment. Any vulnerabilities identified were documented and tracked through to resolution. • "57 - Red Teaming Policy.docx" • "Evidence# 57 - Red Teaming Exercise for AI-170125-175705.pdf"	Compliant	Compliant	
58	We inspected the following: • "KYG_AI_Policy_v2.docx" • "KYG_AI_Transparency_Disclosures_v1.docx" Per inspection, KYG had a responsible AI program in place that covered managing, monitoring, developing and deploying AI solutions.	Compliant	Compliant	
59	We inspected the following: • "KYG_AI_Policy_v2.docx" • "KYG_AI_Transparency_Disclosures_v1.docx" • Screenshot of communicating the transparency disclosure Per inspection, KYG had a transparency disclosure of intended and prohibited uses of their AI systems. The disclosure was updated and communicated to applicable individuals.	Compliant	Compliant	
60	Per inspection of "REQUEST53 KYG_AI_Addendum_v1docx, KYG established contractual terms and agreements to incorporate data handling, confidentiality, intellectual property rights and liability. Per inspection of "Request60_1_EL-Microsoft Pilot.pdf," "Evidence for Contract related language items.pdf" and confirmation with KYG, the AI addendum was communicated to Microsoft and was included in the final agreement.	Compliant	Compliant	
61	We inspected the following: • "KYG_AI_Policy_v2.docx" • "AI Systems Governance Policy.docx" • "AI Org Chart - Deployment and Risk Management Accountability Structure.docx" Per inspection, KYG had defined accountability and responsibilities for the deployment and risk management of AI systems.	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
62	We inspected the following: • "Risk Assessment Policy.docx" • "Request 62 - CAI-Management Review of Risk Assessment - 2025-01-03-070125-044207.pdf" • "Vendor Risk Register.xlsx" Per inspection, KYG conducted a risk assessment on January 3, 2025.	Compliant	Compliant	
63	We inspected the following: • "KYG_AI_Policy_v2.docx" • "AI Systems Governance Policy.docx" • "KYG_AI_Transparency_Disclosures_v1.docx" • "AI System Monitoring & Adaptation Framework.docx" • "Screenshots_AI_Logging_and_Monitoring.docx" Per inspection, KYG had a responsible AI program that ensured developed AI systems were transparent and explainable. KYG monitored and logged system failures, data corruption, hallucinations, misuse or system updates. KYG confirmed that no misuse, deviations or unintended use was noted within the last 12 months.	Compliant	Compliant	
64	We inspected the following: • "KYG_AI_Policy_v2.docx" • "AI System Monitoring & Adaptation Framework.docx" • "Screenshots_AI_Logging_and_Monitoring.docx" • "Request64 Screenshot.docx" Per inspection, KYG had a monitoring and adaptation process in place to continuously monitor and update their AI systems. KYG also maintained log of system failures, data corruption, hallucinations, misuse or system updates.	Compliant	Compliant	
65	We inspected the following: • "KYG_AI_Transparency_Disclosures_v1.docx" • "Screenshots_AI_Logging_and_Monitoring.docx" • "Request64 Screenshot.docx" Per inspection, KYG defined, documented and monitored disclosures that covered error types, acceptable error ranges, performance metric definitions and system performance accordingly.	Compliant	Compliant	

#	Assessment Procedure	Supplier Response	Assessment	Assessor Remarks
66	Per inspection of "KYG_AI_Transparency_Disclosures_v1.docx," KYG included a section about sensitive use, types of updates to the disclosures and the communication process. Transparency disclosures were updated when new use cases were added, functionality changes or new versions were released, and new system performance or risk information was identified. Notifications were sent to customers via email with summary of changes.	Compliant	Compliant	
67	We inspected the following: • "KYG_AI_Transparency_Disclosures_v1.docx" • "AI System Monitoring & Adaptation Framework.docx" • "Screenshots_AI_Logging_and_Monitoring.docx" Per inspection, KYG had a documented monitoring plan for logging and monitoring AI systems.	Compliant	Compliant	
68	We inspected the following: • "KYG_AI_Transparency_Disclosures_v1.docx" • "Screenshots_AI_Logging_and_Monitoring.docx" Per inspection, KYG maintained a list of system health monitoring methods.	Compliant	Compliant	
69	We inspected "KYG_AI_Transparency_Disclosures_v1.docx" and noted that KYG had documented policies and procedures in place that would be followed upon failure of intended use of AI systems. KYG confirmed during the past year, no events was identified suggesting the AI system was not fit for its intended purpose.	Compliant	Compliant	
70	Per confirmation with KYG, KYG did not train or fine-tune any models that involved demographics. KYG only developed AI systems that perform processing on products.	Compliant	Compliant	