Microsoft Supplier Data Protection Requirements

Applicability

The Microsoft Supplier Data Protection Requirements ("**DPR**") apply to each Microsoft supplier that Processes Microsoft Personal Data or Microsoft Confidential Data in connection with that supplier's performance (e.g., provision of services, software licenses, cloud services) under the terms of its contract with Microsoft (e.g., Purchase Order terms, master agreement) ("**Perform,**" "**Performing**" or "**Performance**").

- In the event of a conflict between the requirements contained herein and requirements specified in the contractual agreements between the supplier and Microsoft, the DPR takes precedence unless the applicable supplier identifies in the DPR attestation form the correct provision in the contract that conflicts with the applicable DPR section (in which case, the terms of the contract take precedence).
- In the event of a conflict between the requirements contained herein and any legal or statutory requirements, the legal or statutory requirements take precedence.
- In the event the Microsoft supplier operates as a Controller, with respect to this DPR, only the requirements in section J Security and section A Management apply with respect to that supplier's Processing activities.
- In the event the Microsoft supplier does not Process Microsoft Personal Data but only Microsoft Confidential Data, with respect to this DPR, only the requirements in section A Management, section E Retention, and J Security apply with respect to that supplier's Processing of Microsoft Confidential Data.

International Transfer of Data

Without limiting its other obligations, supplier will not make any international transfer of Microsoft Personal Data unless Microsoft provides prior written approval, and in any event, supplier shall comply with the data protection requirements of any standard contractual terms, binding corporate rules, or other scheme approved by any data protection authority, the European Data Protection Board, or the European Commission and adopted or agreed to by Microsoft, including, the EU-U.S. and Swiss-U.S. Privacy Shield frameworks and the EU General Data Protection Regulation. Supplier agrees to notify Microsoft in the event that Supplier makes a determination that it can no longer meet its obligation to provide the same level of protection as required by the Privacy Shield principles. Supplier shall also ensure that any and all sub processors (as defined in Clause 1(d) of 2010 Standard Contractual Clauses published as an Annex to European Commission Decision C(2010)593) also comply.

Key Definitions

The following terms used in this DPR have the following meanings. List of examples following "including," "such as," "e.g.," "for example," or the like used throughout this DPR are interpreted to include "without limitation," or "but not limited to" unless qualified by words such as "only" or "solely."

"**Controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data; where the purposes and means of Processing are determined by the European Union ("**EU**") or Member State Laws, the controller (or the criteria for nominating the controller) may be designated by those Laws.

"**Data Breach**" means a breach of security leading to the accidental or Unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data or Microsoft Confidential Data transmitted, stored or otherwise Processed.

"**Data Subject Right**" means a Data Subject's right to access, delete, edit, export, restrict, or object to Processing of the Microsoft Personal Data of that Data Subject if required by Law.

"**Law**" means all applicable laws, rules, statutes, decrees, decisions, orders, regulations judgments, codes, enactments, resolutions and requirements of any government authority (federal, state, local, or international) having jurisdiction. "**Unlawful**" means any violation of Law.

"**Microsoft Confidential Data**" is any information which, if compromised through confidentiality or integrity means, can result in significant reputational or financial loss for Microsoft. This includes, Microsoft hardware and software products, internal line-of-business applications, pre-release marketing materials, product license keys, and technical documentations related to Microsoft products and services.

"**Microsoft Personal Data**" means any Personal Data Processed by or on behalf of Microsoft.

"**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Process**" means any operation or set of operations which is performed on any Microsoft Personal Data or Confidential Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Processing" and "Processed" will have corresponding meanings.

"**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section A: Management		
1	Each applicable agreement between Microsoft and the supplier (e.g., master agreement, statement of work, purchase orders and other orders) contains privacy and security data protection language with respect to Microsoft Confidential and Personal Data, as applicable. For companies operating as Processors, the agreement must include the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Microsoft Personal Data and categories of Data Subjects and the obligations and rights of Microsoft.	Supplier must present the applicable contract between Microsoft and Supplier. For Processors, the Processing descriptions are contained in the applicable agreement (*e.g.*, statement of work, purchase orders). Note: Companies with in-flight purchase orders may have the necessary description of Processing activities added later in the purchasing process.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
2	Assign responsibility and accountability for compliance with the DPR to a designated person or group within the company.	Name of the person or group charged with ensuring compliance to the Microsoft Supplier DPR. A document describing the authority and accountability of this person or group that demonstrates a privacy and/or security role.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
3	Establish, maintain, and perform annual privacy and security training for employees that will have access to Microsoft Personal or Confidential Data. If your company does not have prepared content, you can use this storyboard outline and adapt it for your company.	Annual records of attendance are available. Training content includes privacy and security principles.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
4	Process Microsoft Personal Data only in accordance with Microsoft's documented instructions including with regard to transfers of Microsoft Personal Data to a third country or an international organization, unless required to do so by Law; in such a case, the Processor (supplier) shall inform the controller (Microsoft) of that legal requirement before Processing, unless that Law prohibits such information on important grounds of public interest.	Documented evidence of instructions as set out in a contract (e.g. statement of work or purchase order), or captured as part of an electronic system used in Performing.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section B: Notice		
5	The supplier must use the Microsoft Privacy Statement when collecting Personal Data on Microsoft's behalf. The privacy notice must be obvious and available to Data Subjects to help them decide whether to submit their Personal Data to the supplier. Note: Where your company is the Controller of the Processing activity, you would post your own privacy notice. *Contact SSPAHelp@microsoft.com for access to the correct Microsoft notices.*	Supplier uses a fwdlink to the current, published Microsoft Privacy Statement. The Privacy Statement is posted in any context where a user's Personal Data will be collected. If applicable, an offline version is available and is provided prior to data collection. Any offline Privacy Statements used are the latest, published version and are dated properly. For Microsoft employee services, the Microsoft Data Protection Notice is used.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
6	When collecting Microsoft Personal Data via a live or recorded voice call, suppliers must be prepared to discuss the applicable data collection, handling, use, and retention practices with Data Subjects.	A script for voice recordings includes how Microsoft Personal Data is Processed, and includes, ▪ collection, ▪ use and ▪ retention.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section C: Choice and Consent		
7	Where supplier relies on consent as its legal basis for Processing data, the supplier must obtain and record a Data Subject's consent for all of its Processing activities (including any new and updated Processing activities) prior to collecting that Data Subject's Personal Data.	Supplier can demonstrate how a Data Subject provides consent for a Processing activity and that the scope of the consent covers all of supplier's Processing activities with respect to that Data Subject's Personal Data. Supplier can demonstrate how a Data Subject withdraws consent for a Processing activity. Supplier can demonstrate how preferences are checked prior to launch of a new Processing activity. Supplier monitors effectiveness of preference management to ensure the timeframe to honor a preference change is the most restrictive local legal requirement that applies. Note: Evidence can be user interaction screenshots; experimentation with the service or an opportunity to view technical documentation.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section C: Choice and Consent (cont.)		
8	Cookies are small text files stored on devices by websites and/or applications that contain information used to recognize a Data Subject or a device. Suppliers that create and manage Microsoft websites and/or applications must provide Data Subjects with transparent notice and choice regarding the use of cookies. Suppliers that create and manage Microsoft websites and/or applications must ensure that cookie use aligns with commitments in the Microsoft Privacy Statement and local legal requirements such as rules established by the EU.	The purpose of each cookie must be documented and must inform the type of cookie implemented. ▪ Persistent cookies must not be used when session cookies will suffice. ▪ When persistent cookies are used, they must not have an expiration date that exceeds 2 years after a user has visited the site. For EU users, the expiration date for a persistent cookie must not exceed 13 months. Validate compliance with EU Laws as applicable, such as, ▪ use of the labelling convention, “Privacy & Cookies” for the privacy statement, and ▪ secure affirmative user consent before use of cookies for “non-essential” purposes such as advertising.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section D: Collection		
9	The supplier must monitor the collection of Microsoft Personal and/or Confidential Data to ensure that the only data collected is that required to Perform.	Supplier can provide documentation that shows the Microsoft Personal and/or Confidential Data collected is needed to Perform.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
10	If the supplier collects Personal Data from third parties on behalf of Microsoft, the supplier must validate that the third-party data protection policies and practices are consistent with the supplier's contract with Microsoft and the DPR.	Supplier can provide documentation of due diligence performed regarding the third party's data protection policies and practices.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
11	Before collecting Microsoft Personal Data through the installation or utilization of executable software on a Data Subject's device, the necessity for collecting this information must be documented in an executed supplier contract with Microsoft.	Microsoft agreement with the use of executable software on a Data Subject device is noted in the executed contract.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
12	Before collecting sensitive Microsoft Personal Data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) the necessity for collecting that Microsoft Personal Data must be documented in an executed supplier contract with Microsoft.	The necessity of collecting sensitive Microsoft Personal Data is noted in the executed contract with Microsoft.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section E: Retention		
13	Ensure that Microsoft Personal and Confidential Data is retained for no longer than necessary to Perform, unless continued retention of the Microsoft Personal and/or Confidential Data is required by Law.	Supplier complies with documented retention policies or retention requirements specified by Microsoft in the contract (e.g., statement of work, purchase order).	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
14	Ensure that, at Microsoft's sole discretion, Microsoft Personal and Confidential Data in the supplier's possession or under its control is returned to Microsoft or destroyed upon completion of Performance or upon Microsoft's request. Within applications, processes must be in place to ensure that when data is removed from the application either explicitly by users or based on other triggers like the age of the data, that it is securely deleted. When the destruction of Microsoft Personal or Confidential Data is necessary, the supplier must burn, pulverize, or shred physical assets containing Microsoft Personal and/or Confidential Data so that the information cannot be read or reconstructed.	Maintain a record of disposition of Microsoft Personal and Confidential Data (this can include returning to Microsoft for destruction). If destruction is required or requested by Microsoft, provide a certificate of destruction signed by an officer of the supplier.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section F: Data Subjects		
	Data Subjects have rights to access, delete, edit, export, restrict, and object to Processing of their Personal Data ("**Data Subject Rights**"). When a Data Subject seeks to exercise their rights under Law in respect of their Microsoft Personal Data, the supplier must:		
15	Assist Microsoft, through appropriate technical and organizational measures, insofar as possible, to fulfill its obligations to respond to requests for Data Subjects seeking to exercise their Data Subject Rights.	Processes and procedures are in place to support execution of Data Subject Rights.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
16	Respond to all Data Subject Rights requests without undue delay.	Supplier conducts periodic tests to ensure they can support Data Subject Rights.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
17	Unless otherwise directed by Microsoft, Supplier will refer all Data Subjects who contact Supplier directly to Microsoft to exercise their Data Subject Rights. Supplier will communicate to the Data Subject the steps that person must take to gain access to or otherwise exercise their rights vis-à-vis their Microsoft Personal Data. *Contact SSPAHelp@microsoft.com for help with this requirement.*	Supplier communicates the steps to be taken to access the Personal Data, as well the methods available to update that data.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
18	When responding directly to the Data Subject, validate the identity of the Data Subject making the request.	Supplier has documented the method used to identify Microsoft Data Subjects.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section F: Data Subjects (cont.)		
	Once a Data Subject has been authenticated, the supplier must:		
19	Determine whether it holds or controls Microsoft Personal Data about that Data Subject.	Supplier has procedures in place to establish whether Personal Data is being held.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
20	Make a reasonable effort to locate the Microsoft Personal Data requested and keep sufficient records to demonstrate that a reasonable search was made.	Supplier maintains a record demonstrating the steps taken to meet Data Subject Right requests. The documentation includes, ▪ date and time of the request, ▪ actions taken to respond to the request, and ▪ record of when Microsoft was informed.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
21	Record the date and time of Data Subject Rights requests and the actions taken by supplier in response to such requests. Provide records of Data Subject requests to Microsoft upon request.	Supplier maintains records of requests for access and documents changes made to Personal Data.	
	Once a Data Subject has been authenticated and the supplier has validated that they have the Microsoft Personal Data requested, the supplier must:		
22	For requests to obtain a copy of Personal Data, provide the Microsoft Personal Data to the Data Subject in an appropriate printed, electronic or verbal format.	Supplier supplies Personal Data to the Data Subject in a format that is understandable and in a form convenient to the Data Subject and the supplier.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
23	If their request is denied, at Microsoft's direction, provide the Data Subject with a written explanation that is consistent with any relevant instructions previously provided by Microsoft. *Contact SSPAHelp@microsoft.com for help with this requirement.*	Document instances where requests are denied and retain evidence of Microsoft review and approval.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence Required	Response
	Section F: Data Subjects (cont.)		
24	The supplier must take reasonable precautions to ensure that Microsoft Personal Data released to a Data Subject cannot be used to identify another person.	Supplier must demonstrate that reasonable precautions are taken so that another person cannot be identified from the information released (e.g., cannot photocopy the entire page of data when requested Personal Data for a Data Subject only appears on one line).	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
25	If a Data Subject and a supplier disagree about whether Microsoft Personal Data is complete and accurate, the supplier must escalate the issue to Microsoft and cooperate with Microsoft as necessary to resolve the issue. *Contact SSPAHelp@microsoft.com for help with this requirement.*	Supplier documents instances of disagreement and escalates issue to Microsoft.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section G: Disclosure to Third Parties		
	If the supplier intends to use a subcontractor to Process Microsoft Personal or Confidential Data, the supplier must:		
26	Obtain Microsoft's express written consent prior to subcontracting services or making any changes concerning the addition or replacement of subcontractors. *Contact SSPAHelp@microsoft.com for help with this requirement.*	Validate that Microsoft Personal Data is Processed only by companies known to Microsoft as required in the applicable contract (e.g., statement of work, addendum, purchase order) or captured in the SSPA database.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
27	Document the nature and extent of Microsoft Personal and Confidential Data sub-Processed by subcontractors, ensuring that the information collected is required to Perform.	Supplier maintains documentation concerning the Microsoft Personal and Confidential Data disclosed or transferred to subcontractors.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
28	Ensure the subcontractor uses Microsoft Personal Data in accordance with a Data Subject's stated contact preferences.	Demonstrate how a Microsoft Data Subject preference is utilized by subcontractors. Provide supporting documentation that includes the timeframe for a subcontractor to honor a preference change.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
29	Limit the subcontractor's Processing of Microsoft Personal Data to those purposes necessary to fulfill the supplier's contract with Microsoft.	Supplier can provide documentation that shows the Microsoft Personal Data provided to a subcontractor is needed to Perform.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
30	Review complaints for indications of any unauthorized or Unlawful Processing of Microsoft Personal Data.	Supplier can demonstrate systems and processes are in place to address complaints concerning unauthorized use or disclosure of Microsoft Personal Data by a subcontractor.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
31	Notify Microsoft promptly upon learning that a subcontractor has Processed Microsoft Personal or Confidential Data for any purpose other than those related to Performance.	Supplier has provided the instruction and means for a subcontractor to report the misuse of Microsoft data.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section G: Disclosure to Third Parties (cont.)		
32	Promptly take actions to mitigate any actual or potential harm caused by a subcontractor's unauthorized or Unlawful Processing of Microsoft Personal and Confidential Data.	Supplier can demonstrate they have a plan and procedures in place should the misuse of Microsoft Personal and Confidential Data by a subcontractor occur.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
	Section H: Quality		
33	The supplier must maintain the integrity of all Microsoft Personal Data, ensuring it remains accurate, complete and relevant for the stated purposes for which it was Processed.	Supplier can demonstrate that procedures are in place to validate Microsoft Personal Data when it is collected, created and updated. Supplier can demonstrate that monitoring and sampling procedures are in place to verify accuracy on an on-going basis and correct as necessary.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section I: Monitoring and Enforcement		
34	Supplier has an incident response plan that requires Supplier to notify Microsoft without undue delay upon becoming aware of a Data Breach or security vulnerability related to the supplier's handling of Microsoft Personal or Confidential Data. *Contact SSPAHelp@microsoft.com to report an incident.*	Supplier has an incident response plan which includes a step to notify customers (Microsoft) as described in this section.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
35	Not issue any press release or any other public notice that relates to a Data Breach involving Microsoft Personal or Confidential Data without getting Microsoft approval, unless expressed by Law.	Supplier agrees to fulfill this requirement if the event occurs.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
36	Implement a remediation plan and monitor the resolution of Data Breaches and vulnerabilities related to Microsoft Personal or Confidential Data to ensure that appropriate corrective action is taken on a timely basis.	Supplier has documented procedures it will take to respond to a Data Breach to closure.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
37	Establish a formal complaint process for responding to all data protection complaints involving Microsoft Personal Data.	Supplier has the means of receiving complaints involving Microsoft Personal Data and has a documented complaint procedure to address complaints.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security		
	The supplier must establish, implement, and maintain an information security program that includes policies and procedures, to protect and keep secure Microsoft Personal and Confidential Data in accordance with good industry practice and as required by Law. The supplier's security program must meet the standards captured below, requirements 38 -56.	Safeguards may exceed those listed, as necessary to meet regulatory schemes (e.g., HIPAA, GLBA) or contractual requirements. A valid ISO 27001 or SOC 2 report with security are acceptable substitutes for Section J. Contact SSPAHelp@microsoft.com to apply this substitution. Note: You will need to provide documentation describing the scope of these certifications/reports.	
38	Perform annual network security assessments that includes, ▪ review of major changes to the environment such as a new system component, network topology, firewall rules, ▪ conduct vulnerability scans, and ▪ maintain change logs.	Supplier has documented network assessments, change logs and scan results. The required change logs must track changes, provide information regarding the reason for the change, and include the name and title of the designated approver.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
39	Supplier to define, communicate and implement a mobile device policy that secures and limits use of Microsoft Personal or Confidential Data accessed or used on a mobile device.	Supplier demonstrates use of a compliant mobile device policy where Microsoft Personal or Confidential Data Processing requires use of a mobile device.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
40	All assets used to support Performance must be accounted for and have an identified owner. The supplier is accountable for maintaining an inventory of these information assets; establishing acceptable and authorized use of the assets; and providing the appropriate level of protection for the assets throughout their life cycle.	Inventory of device assets used to support Performance. The inventory of these assets to include, ▪ location of device, ▪ data classification of the data on the asset, ▪ record of asset recovery upon termination of employment or business agreement, and ▪ record of disposal of data storage media when it's no longer required.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
41	Establish and maintain access rights management procedures to prevent unauthorized access to any Microsoft Personal or Confidential Data under supplier control.	Supplier demonstrates it has implemented an access rights management plan that includes, ▪ access control procedures, ▪ identification procedures, ▪ lockout procedures after unsuccessful attempts, ▪ password reset as often as necessary but no longer than every 90 days, ▪ robust parameters for selecting authentication credentials, and ▪ deactivation of user accounts on employment termination within 48 hours. Supplier demonstrates that it has an established process to review user access to Microsoft Personal and Confidential Data, enforcing the principle of least privilege. The process includes, ▪ clearly defined user roles, ▪ procedures to review and justify approval of access to roles, and ▪ test that users within roles with access to Microsoft data have a documented justification for being in the group/role.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
42	Define and implement patch management procedures that prioritize security patches for systems used to Process Microsoft Personal or Confidential Data. These procedures include, ▪ defined risk approach to prioritize security patches ▪ ability to handle and implement emergency patches, ▪ applicability to Operating System and server software such as application server and database software, ▪ document the risk the patch mitigates and track any exceptions, and ▪ requirements for retirement of software that is no longer supported by the authoring company.	Supplier can demonstrate an implemented patch management procedure that meets this requirement and covers, at a minimum, the following. ▪ Assignment of severity to inform prioritization. (Severity definitions are documented.) ▪ Documented procedure to implement emergency patches. ▪ Validate, there is no use of operating systems that are no longer supported by the authoring company. ▪ Patch management records which track approvals and exceptions.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
43	Install anti-virus and anti-malware software on equipment connected to the network used to Process Microsoft Personal and Confidential Data, including servers, production and training desktops to protect against potentially harmful viruses and malicious software applications. Update the anti-malware definitions daily or as directed by the anti-virus/anti-malware supplier. Note: This applies to all operating systems including Linux.	Records exist to show use of anti-virus and anti-malware software is active. Note: This requirement applies to all operating systems.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
44	Suppliers developing software for Microsoft must incorporate security-by-design principles in the build process.	Supplier technical specification documents include check points for security validation in their development cycles.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
45	Employ a Data Loss Prevention ("**DLP**") program. Data must be properly classified, labeled and protected and supplier must monitor information systems in use where Microsoft Personal or Confidential Data is Processed for intrusions, loss, and other unauthorized activity. The DLP program, at a minimum, ▪ requires use of industry standard host, network, and cloud-based Intrusion Detection Systems ("**IDS**") if you retain Microsoft Personal or Confidential Data, ▪ requires implementation of advanced Intrusion Protection Systems ("**IPS**") configured to monitor and actively stop data loss, ▪ in the event a system is breached, requires analysis of the system to ensure any residual vulnerabilities are also addressed, ▪ describe required procedures for monitoring system compromise detection tools, and ▪ establishes an incident response and management process required to be performed when a Data Breach events is detected.	Documented IDS/IPS deployed with procedures in place to direct response when a vulnerability or Data Breach is detected.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
46	Promptly communicate Investigation results from incident response to senior management and to Microsoft. *Contact SSPAHelp@microsoft.com to inform Microsoft.*	Systems and processes must be in place to communicate incident response investigation results to Microsoft.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*
47	System administrators, operations staff, management and third parties must undergo annual security training.	Establish a security training program that includes, ▪ annual training for incident response, and ▪ simulated events and automated mechanisms to facilitate effective response to crisis situations. Incident prevention awareness such as risks associated with downloading malicious software.	*<Compliant> <Not Compliant> <Does not Apply> <Legal Conflict> <Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
48	The supplier must ensure that backup planning processes protect Microsoft Personal and Confidential Data from unauthorized use, access, disclosure, alteration and destruction.	Supplier can demonstrate documented response and recovery procedures detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level based on management approved information security continuity objectives. Supplier can demonstrate that it has defined and implemented procedures to periodically back up, securely store, and effectively recover critical data.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
49	Establish and test business continuity and disaster recovery plans.	A disaster recovery plan must include all of the following. ▪ Defined criteria to determine if a system is critical to the operation of the supplier's business. ▪ List critical systems based on the defined criteria that must be targeted for recovery in the event of a disaster. ▪ Defined disaster recovery procedure for each critical system that ensures an engineer who does not know the system could recover the application in under 72 hours. ▪ Annual (or more frequent) testing and review of disaster recovery plans to ensure recovery objectives can be met.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
50	Authenticate the identity of an individual before granting that individual access to Microsoft Personal or Confidential Data.	Ensure that all user IDs are unique and that each has an industry standard authentication method such as Azure Active Directory. Elevated access (administrative or other types of enhanced privileges) must require the use of a second factor, such as a smart card or phone based authenticator.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
51	The supplier must protect Microsoft Personal and Confidential Data in transit across networks with encryption using Transport Layer Security ("**TLS**") or Internet Protocol Security ("**IPsec**"). These methods are described in the NIST 800-52 and NIST 800-57; an equivalent industry standard can also be used. Supplier must refuse delivery of any Microsoft Personal or Confidential Data transmitted via unencrypted means.	The process of creating, deploying, and replacing TLS or other certificates must be defined and enforced.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
52	All supplier devices (laptops, workstations, etc.) that will access or handle Microsoft Personal or Confidential Data must employ disk based encryption.	Encrypt all devices to meet Bitlocker or another industry equivalent disk encryption solution for all client devices used to handle Microsoft Personal or Confidential Data.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance	Response
	Section J: Security (cont.)		
53	Systems and procedures (using current industry standards such as that described in the NIST 800-111 standard) must be in place to encrypt at rest (when stored) any and all Microsoft Personal and/or Confidential Data, including any and all of the following: ▪ credential data (e.g., username/passwords) ▪ payment instrument data (e.g., credit card and bank account numbers) ▪ immigration related personal data ▪ medical profile data (e.g., medical record numbers or biometric markers or identifiers, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, used for authentication purposes) ▪ government issued identifier data (e.g., social security or driver's license numbers) ▪ data belonging to Microsoft customers (e.g., Sharepoint, O365 documents, One drive customers) ▪ material related to unannounced Microsoft products ▪ Date of Birth ▪ Children's profile information ▪ real time geographic data ▪ physical personal (non-business) address ▪ personal (non-business) phone numbers ▪ religion ▪ political opinions ▪ sexual orientation/preference ▪ security question answers (e.g., 2fa, password reset) ○ mother's maiden name	Check that the Microsoft Personal and Confidential Data listed in this row is encrypted at rest.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
54	When processing credit cards on Microsoft's behalf, adhere to the applicable credit card handling standards per card issuer.	Demonstrate compliance by providing a Payment Card Industry Data Services Standard ("**PCI-DSS**") certification annually. *Submit PCI DSS certifications to SSPA. Please contact SSPAHelp@microsoft.com* with any questions.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*

#	Microsoft Supplier Data Protection Requirements	Evidence Required	Response
	Section J: Security (cont.)		
55	The supplier must store Microsoft physical assets in an access-controlled environment.	Systems and processes must be in place to manage physical access to digital, hard copy, archival, and backup copies of Microsoft data. Chain of custody must be tracked for the movement and destruction of physical media containing Microsoft data.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*
56	Anonymize all Microsoft Personal Data used in a development or test environment.	Microsoft Personal Data must not be used in development or test environments; when there is no alternative, it must be anonymized to prevent identification of Data Subjects or misuse of Personal Data. Note: Anonymized data is different from Pseudonymized data. Anonymized data is data that does not relate to an identified or identifiable natural person where the data subject of the personal data is not or no longer identifiable.	*<Compliant>* *<Not Compliant>* *<Does not Apply>* *<Legal Conflict>* *<Contract Conflict>*