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 DPR and requirements specified in the contractual agreements between the supplier and Microsoft, the DPR takes precedence unless the supplier identifies the correct provision in the contract that supersedes the applicable data protection requirement (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, supplier may have reduced requirements in the DPR.
- In the event the Microsoft supplier does not Process Microsoft Personal Data but only Microsoft Confidential Data, with respect to this DPR, supplier may have reduced requirements.

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, including the Standard Contractual Clauses, or, at Microsoft's discretion, other appropriate cross-border transfer mechanisms approved by an appropriate data protection authority or the European Commission, as applicable, and adopted or agreed to by Microsoft. Successor Standard Contractual Clauses adopted by (i) the European Commission or adopted by the European Data Protection Supervisor and approved by the European Commission, (ii) the United Kingdom pursuant to the UK General Federal Data Protection Act, (iii) Switzerland pursuant to the Swiss Federal Data Protection Act, or (iv) clauses governing the international transfer of personal data officially adopted by a government in a jurisdiction other than Switzerland, the United Kingdom, and the jurisdictions comprising the European Union / European Economic Area, shall be incorporated and binding on Supplier as of the day of their adoption. Supplier shall also ensure that any and all sub processors (as defined in the Standard Contractual Clauses) 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." For further definitions, please see the Glossary at the end of this document.

"**Controller"** means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes a Business, Controller (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

"**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.

"**Data Incident**" means (1) a breach of security leading to the accidental or Unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Microsoft Personal Data or Microsoft Confidential Data transmitted, stored or

otherwise Processed by Supplier or its Subcontractors, or (2) security vulnerability related to Supplier's handling of Microsoft Personal Data or Microsoft Confidential Data or confidentiality incident as defined under Bill 64 (2021, chapter 25).

"**Data Subject**" means an identifiable natural person who can be identified, directly or indirectly, in particular by referencing 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.

"**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 a Data Subject and any other information that constitutes "personal data" or "personal information" under Law.

"**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 an entity that Processes Personal Data on behalf of another entity and includes Service Provider, Processor (as that term is defined in the GDPR), and equivalent terms in Data Protection Laws, as context requires.

"**Protected Health Information**" or "**PHI**" means Microsoft Personal Data that is protected by the Health Information Portability and Accountability Act (HIPAA).

"**Subcontractor**" means a third-party to whom supplier delegates its obligations in connection with the contract covering their Performance, including a supplier affiliate not contracting directly with Microsoft.

"**Subprocessor**" means a third party that Microsoft engages to Perform, where the Performance includes Processing of Microsoft Personal Data for which Microsoft is a Processor.

Supplier Response

Suppliers confirm compliance to these requirements annually using an online service administered by Microsoft. Please see the SSPA Program Guide to understand how compliance is administered.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	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, including prohibitions on the sale of Microsoft Personal Data and Processing of Microsoft Personal Data outside the direct business relationship between Microsoft and supplier. For companies operating as Processors or Subprocessors in connection with the Performance, with respect to Microsoft Personal Data, 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 and Subprocessors, 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.
2	Where Microsoft confirms that your engagements fulfill a Subprocessor role, Supplier must have applicable data protection agreements in place with Microsoft. If Microsoft confirms that your engagements involve the processing of PHI, Supplier must have a Business Associate Agreement and/or other agreement in place with Microsoft. Note: Microsoft will post these designations to your profile when they apply.	Standard Contractual Clauses, Online Customer Data Addendum, Supplier and Partner Professional Services Data Processing Addendum and/or Business Associate Agreement.
3	Assign responsibility and accountability for compliance with the DPR to a designated person or group within the company.	Name the role 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.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section A: Management (cont.)	
4	Establish, maintain, and perform annual privacy and security training for employees that will have access to Personal Data Processed by supplier in connection with Performance or Microsoft Confidential Data. If your company does not have prepared content, you can use this storyboard outline and adapt it for your company. Note: Supplier personnel may be required to complete additional trainings provided by Microsoft divisions.	Annual records of attendance are available and can be provided to Microsoft upon request. Training content includes privacy and security principles. If the Microsoft Personal Data Processed by supplier includes PHI, training content must include HIPAA training, including supplier's permitted uses and disclosures as permitted by the Business Associate Agreement. Documentation of compliance with training requirements will include evidence of training related to privacy regulatory requirements, security obligations, and compliance with applicable contract requirements and obligations.
5	Apply appropriate sanctions against employees who fail to comply with supplier's privacy and security policies.	Documentation of privacy and security policies that describe sanctions for non-compliance (e.g., up to and including termination).
6	Process Microsoft Personal Data only in accordance with Microsoft's documented instructions including scenarios 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 or Subprocessor (supplier) shall inform the Controller (Microsoft) of that legal requirement before Processing, unless that Law prohibits such information on important grounds of public interest.	Supplier compiles and maintains all Microsoft documented instructions (e.g., agreements, statement of work or order documentation) and its privacy and security policies and procedures electronically, in an easily accessible location to supplier's employees and contractors participating in the Performance.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section B: Notice	
7	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.	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 Privacy Notice is used.
8	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
	Section C: Choice and Consent	
9	Where applicable, 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 monitors effectiveness of preference management to ensure the timeframe to honor a preference change is the most restrictive local legal requirement that applies.	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. Note: Evidence can be user interaction screenshots; experimentation with the service or an opportunity to view technical documentation.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section C: Choice and Consent (cont.)	
10	Suppliers that create and manage Microsoft websites and/or applications or sites that carry Microsoft branding must provide Data Subjects with transparent notice and choice regarding the use of cookies in alignment with commitments in the Microsoft Privacy Statement and local legal requirements. Unless specifically requested not to by the contracting business unit, suppliers should use the Standard Banner produced by 1ES to manage choice controls. This requirement applies when sites target users within the European Union/European Economic Area and other regions with applicable privacy laws and wherever the Microsoft Privacy Statement is used. Note: Microsoft business sponsors are required to register Microsoft websites in the internal Web Compliance portal (http://aka.ms/wcp) to have the inventory of cookies cataloged and managed.	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 suffice. ▪ When persistent cookies are used, they must not have an expiration date that exceeds 13 months after a user has visited the site. Validate compliance with EU Laws as applicable, such as: ▪ use of the labelling convention, "Privacy & Cookies" ▪ for the privacy statement, ▪ secure affirmative user consent before use of "non- essential" cookies for purposes such as advertising, and ▪ consent must expire or be re-obtained no longer than every 6 months.
	Section D: Collection	
11	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. Supplier will furnish documentary evidence to Microsoft upon request.
12	Before collecting data from children (as defined by applicable jurisdiction), Supplier must obtain the consent per local privacy laws.	Supplier can provide documentation that shows parent/guardian consent. Supplier will furnish documentary evidence to Microsoft upon request.
13	Where supplier receives a data set from Microsoft with reduced identifiability, including pseudonymous, Not in a Position to Identify (NPI), unlinked pseudonymous, aggregate, anonymous, or any term that relates to one of those classifications (such as de-identified), supplier will maintain the data in the state in which it was received.	Supplier will not increase the identifiability of data sets (i.e. reidentify individuals who are part of a data set through joining to other data sets, etc.). Supplier has a de-identification/anonymization data policy/process.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section E: Retention	
14	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). Supplier will furnish documentary evidence to Microsoft upon request.
15	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.
	Section F: Data Subjects	
	Data Subjects have certain rights under Law, including the right 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 enable Microsoft to do the following or perform these actions on Microsoft's behalf:	
16	Assist Microsoft, through appropriate technical and organizational measures, where possible, to fulfil its obligations to respond to requests for Data Subjects seeking to exercise their Data Subject Rights without undue delay. 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 maintain evidence of documented processes and procedures to support Data Subject Rights execution. Supplier will maintain documented evidence of testing. Evidence will be available upon request by Microsoft.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section F: Data Subjects (cont.)	
17	When responding directly to the Data Subject or when the Supplier provides a self-service online mechanism, the Supplier has processes and procedures in place to identify the Data Subject making the request.	Supplier has documented the method used to identify Microsoft Data Subjects. Supplier will provide documented evidence to Microsoft upon request.
18	If asked by Microsoft to locate Microsoft Personal Data about a Data Subject that is not available through a self-service online mechanism, the Supplier will make a reasonable effort to locate the data requested and keep sufficient records to demonstrate that a reasonable search was made.	Supplier will maintain documented evidence of procedures in place to establish whether Microsoft Personal Data is being held and will provide documentation to Microsoft upon request. 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. Supplier will provide evidence of record keeping to Microsoft upon request.
19	Supplier will communicate to the Data Subject the steps that person must take to gain access to or otherwise exercise their rights in regard to their Microsoft Personal Data.	Supplier will maintain documented evidence of the communications and procedures for access to Microsoft Personal Data. Supplier will maintain documented evidence and furnish same evidence to Microsoft upon request.
20	Record the date and time of Data Subject Rights requests and the actions taken by supplier in response to such requests. If their request is denied, at Microsoft's direction, provide the Data Subject with a written explanation. Provide records of Data Subject requests to Microsoft upon request.	Supplier maintains records of requests for access/deletion and documents changes made to Microsoft Personal Data. Document instances where requests are denied and retain evidence of Microsoft review and approval. Supplier will furnish evidence of record keeping of requests and denials of access to Microsoft Personal Data.
21	The supplier must enable Microsoft or obtain a copy of the requested Microsoft Personal Data for the authenticated Data Subject in an appropriate printed, electronic or verbal format.	Supplier supplies Microsoft Personal Data to the Data Subject in a format that is understandable and in a form convenient to the Data Subject and the supplier.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section F: Data Subjects (cont.)	
22	The supplier must take reasonable precautions to ensure that Microsoft Personal Data released to Microsoft or an authenticated Data Subject cannot be used to identify another person.	Supplier will maintain documented evidence of procedures related to precautions to avoid identification of Data Subject contrary to Agreement terms. Supplier will furnish evidence to Microsoft upon request.
23	If a Data Subject believes their Microsoft Personal Data is not complete and accurate, the supplier must escalate the issue to Microsoft and cooperate with Microsoft as necessary to resolve the issue.	Supplier documents instances of disagreement and escalates the issue to Microsoft. Supplier will furnish Microsoft with documentary evidence upon request.
	Section G: Subcontractors	
	If the supplier intends to use a subcontractor to Process Microsoft Personal or Confidential Data, the supplier must:	
24	Notify Microsoft prior to subcontracting services or making any changes concerning the addition or replacement of subcontractors. Note: Indicate your acceptance of this obligation even if you do not currently engage subcontractors but may in the future.	Validate that Microsoft Personal and/or Confidential 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. Supplier may post their subcontractor list online and include a link to the page in the SSPA database.
25	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. Supplier will furnish documentary evidence to Microsoft upon request.
26	Where Microsoft is a Controller of Microsoft Personal Data, 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 (e.g., screenshot, SLA, SOW, etc.) that includes the timeframe for a subcontractor to honor a preference change.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section G: Subcontractors (cont.)	
27	Limit the subcontractor's Processing of Microsoft Personal or Confidential Data to those purposes necessary to fulfill the supplier's contract with Microsoft. If the Microsoft Personal Data is PHI, also enter into a Business Associate Agreement with the subcontractor that limits the subcontractor's Processing of the Microsoft Personal Data and protects the confidentiality and security of the Microsoft Personal Data in the same manner as the Business Associate Agreement between Microsoft and Supplier.	Supplier can provide documentation that shows the Microsoft Personal Data provided to a subcontractor is needed to Perform. Supplier will furnish documentary evidence to Microsoft upon request, including a Business Associate Agreement, if applicable.
28	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. Supplier will furnish documentary evidence to Microsoft upon request.
29	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. Supplier will furnish documentary evidence to Microsoft upon request.
30	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. Supplier will furnish documentary evidence to Microsoft upon request.
31	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 must maintain documentary evidence of plan and procedure and furnish evidence of documentation to Microsoft upon request.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section H: Quality	
32	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, review of information system activity and sampling procedures are in place to verify accuracy on an on-going basis and correct, as necessary. Supplier will furnish documentary evidence to Microsoft upon request.
	Section I: Monitoring and Enforcement	
33	Supplier has an incident response plan that requires Supplier to notify Microsoft per contractual requirements or without undue delay, whichever is sooner, upon becoming aware of a Data Incident. Supplier must at Microsoft's request or direction, cooperate with Microsoft in any investigation, mitigation, or remediation of the Incident, including providing Microsoft with data, information, access to Supplier personnel, or hardware needed to conduct a forensic review. Note: Please see the SSPA Program Guide for how to notify Microsoft of an incident.	Supplier has an incident response plan which includes a step to notify customers (Microsoft) as described in this section. Supplier will furnish documentary evidence to Microsoft upon request.
34	Implement a remediation plan and monitor the resolution of each Data Incident to ensure that appropriate corrective action is taken on a timely basis.	Supplier has documented procedures it will take to respond to a Data Incident to closure. Supplier will furnish documentary evidence to Microsoft upon request.
35	Where Microsoft is a Controller of Microsoft Personal Data, 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. Supplier will furnish documentary evidence to Microsoft upon request.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	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 36 -52. If the Microsoft Personal Data is PHI, the supplier must also perform a periodic technical and non-technical evaluation in response to environmental and operational changes affecting the security of PHI that establishes the extent to which the supplier's policies and procedures meet the requirements of the HIPAA Security Rule.	A valid ISO 27001 Certification is an acceptable substitute for Section J. Contact SSPA to apply this substitution. Note: You will need to provide the certification.
36	Perform annual network security assessments that include: ▪ assessing the potential risks and vulnerabilities to the confidentiality, integrity and availability of Microsoft Personal Data and the implementation of measures to reduce risks, ▪ reviewing of major changes to the environment such as a new system component, network topology, firewall rules, ▪ maintaining 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.
37	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.
38	All physical and virtual assets used to support Performance, security, and operations 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, security, and operations. 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 is no longer required.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
39	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, ▪ automatic logoff after inactivity ▪ robust parameters for selecting authentication credentials, and ▪ deactivation of user accounts (including accounts used by employees or subcontractors) on employment or termination within 48 hours ▪ strong password controls that enforce password length and complexity and prevent reuse 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.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
40	Define and implement patch management procedures that prioritize security patches for systems used to Process Microsoft Personal or Confidential Data. These procedures include: ▪ conduct vulnerability scans on a monthly basis with high level compliance report showing monthly scans for the prior 12 months ▪ 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.
41	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. The anti-virus and anti-malware software should be regularly patched and up-to-date. 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.
42	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.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
43	Employ a Data Loss Prevention ("DLP") program to prevent intrusions, loss, and other unauthorized activity at the application, system, and infrastructure levels. 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, ▪ establishes an incident response and management process required to be performed when a Data Incident is detected, and ▪ requires communications (to all supplier employees and subcontractors being offboarded from ▪ supplier's Performance) regarding unauthorized downloading and use of Microsoft Personal or Confidential Data.	Documented DLP program deployed with procedures in place to prevent intrusions, loss, and other unauthorized activity (and at a minimum, all items specified in this section).

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
44	Promptly communicate Investigation results from incident response to senior management and to Microsoft.	Systems and processes must be in place to communicate incident response investigation results to Microsoft.
45	System administrators, operations staff, management third parties, and anyone accessing Microsoft Personal or Confidential Data must undergo annual security training.	Establish an annual security training program that includes: ▪ Training for incident response, and simulated events and automated mechanisms to facilitate effective response to crisis situations. ▪ Incident prevention awareness including safeguarding passwords, log-in monitoring, risks associated with downloading malicious software, and other relevant security reminders. ▪ If the Microsoft Personal Data is PHI, the awareness and training program must include security reminders and address log-in monitoring and safeguarding passwords. ▪ Content that is regularly updated
46	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.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
47	Establish and test business continuity and disaster recovery plans.	A disaster recovery plan must include 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.
48	Authenticate the identity of an individual before granting that individual access to Microsoft Personal or Confidential Data and ensure that the access is limited to the particular individual's scope of activity permitted to support Performance.	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. Documented information security program covering process for ensuring that all supplier employees' and subcontractors' access to Microsoft Personal or Confidential Data is no more or longer than necessary to support Performance.
49	The supplier must protect all data Processed in connection with its Performance 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.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
50	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.
51	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, examples include, but are not limited to: ▪ 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, OneDrive 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 is encrypted at rest.

#	Microsoft Supplier Data Protection Requirements	Evidence of Compliance
	Section J: Security (cont.)	
52	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. If the Microsoft Personal Data is PHI, the anonymization must meet the HIPAA de-identification standard.
53	Supplier to ensure that secrets are not embedded or hardcoded in the software at any stage of the development process.	Supplier has documented procedures for ensuring that secrets such as usernames, passwords, SSH keys, API access tokens, etc., were never incorporated into source or configuration files, either in test or production environments. Supplier can demonstrate: ▪ use of a supported and current version of a credential exposure prevention tool such as GitHub Advanced Security (GHAS)) or similar service or tool. ▪ assurance that if source or configuration files did mistakenly include secrets, those secrets were documented as revoked upon discovery. ▪ assurance that any replacement or secondary credential was not pushed back into code. ▪ documentation of any false positives and their remediation.

Glossary

“Authorized Representative” is a person that has the appropriate level of authority to sign on behalf of the company. This person would have the requisite privacy and security knowledge or have consulted a subject matter expert prior to submitting their response to an SSPA Program action. In addition, by adding their name to a SSPA form they are certifying that they have read and understand the DPR.

“EUDPR” means Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC.

"Freelancer" means individuals performing on-demand tasks or services, which are procured through digital platforms or other means.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Privacy Data Protection Requirements” means the GDPR, the EUDPR, Local EU/EEA Data Protection Laws, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (“*CCPA*”), the UK Data Protection Act 2018 and any related or subsequent laws, regulations and other legal requirements applicable in the UK, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; or (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

“EU Model Clauses” and “Standard Contractual Clauses” mean (i) the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision (EU) 2021/914 of 4 June 2021; (ii) any successor standard contractual clauses adopted by (a) the European Commission, (b) the European Data Protection Supervisor and approved by the European Commission, (c) the United Kingdom pursuant to the UK General Federal Data Protection Act, (d) Switzerland pursuant to the Swiss Federal Data Protection Act, or (e) by a government in a jurisdiction other than Switzerland, the United Kingdom, and the jurisdictions comprising the European Union / European Economic Area where the clauses govern the international transfer of personal data, shall be incorporated and binding on Supplier as of the day of their adoption.

“Website Hosting” A website hosting service is an online service that creates and/or maintains websites on behalf of Microsoft under the Microsoft domain, i.e., supplier provides all materials and services required for them to create and maintain a site and makes it accessible on the internet. The “web hosting service provider” or “web host” is the supplier who provides the tools and services needed for the website or webpage to be viewed on the Internet, such as, Cookies or web beacons for advertising.