SSPA Independent Assessment Report Template (v10 DPR)

Supplier Security & Privacy Assurance (SSPA)

Microsoft Procurement

Microsoft

Introduction

The SSPA Program Guide is your comprehensive resource for all aspects of the SSPA program, including qualifications for assessors and detailed instructions on completing the Independent Assessment requirement. Before attempting to complete the assessment, please review the instructions below and the Independent Assessment section within the guide. Familiarizing yourself with the program and these instructions will help ensure your assessment is completed correctly and not returned due to errors.

Please contact the SSPA support team at SSPAHelp@microsoft.com for help with the Independent Assessment requirement.

Scope

The scope of the engagement is limited to all in-scope data processing activity executed against the supplier account number which received the request. If the supplier elects to review more than one supplier account at one time, the letter of assessment must include the list of supplier accounts included in the assessment.

The letter submitted to SSPA must not include any statements where the supplier cannot meet the Data Protection Requirements as written. These issues must be corrected before the letter is submitted.

Instructions

It's important to note that the assessor's role is not to determine applicability, but to validate the accuracy of the supplier's self-attestation.

- **If the supplier marks the requirement as 'compliant,'** your assessment should focus on gathering evidence from the evidence of compliance column to confirm compliance.
- **If the supplier marks the requirement as 'Does Not Apply,'** your assessment should involve reviewing the supplier's contracts, purchase orders, and/or statements of work to validate their claim. Rather than making a decision about applicability, the assessor's responsibility is to verify that the supplier's statements align with their contractual obligations and to ensure the self-attestation is accurate.

1. **Ensure You Are Assessing the Supplier's Most Recent, Accepted, Self-Attestation**: Verify with the supplier, that you have the latest accepted Self-Attestation from the supplier.
2. **Assessment Table Template**: Ensure your Assessment Report matches the DPR requirements completed by the supplier. SSPA will not accept assessments that do not match the correct DPR.
    - **Assessment Table should be on the Assessing Company's Letterhead**: Ensure that the assessment table is placed on the assessing company's official letterhead. Assessments will not be accepted if not on the Assessing Company's letterhead.
    - **Do Not Make Any Changes to the Column Formatting**: Maintain the original formatting of the assessment table columns.
    - **Remove Unassigned Requirements**: You may remove any requirements which were not assigned to your supplier. *Example Req#2 only will appear if the supplier is an approved Subprocessor.*

3. **Enter the Supplier's Name and Account Number**: Enter the supplier's name and account number. If there is more than one supplier account, please list all of the applicable accounts numbers the assessment is for. Note: SSPA will not apply this assessment to any account which is not listed within the table.
4. **In the Supplier Response Column:** Enter the supplier's DPR responses.
5. **In the Assessor Response Column**: Complete the assessment for each requirement. Specifically, ensure the criteria within the requirement and evidence of compliance are met. **Use the following entries ONLY**:
    - **Compliant**: Supplier is compliant to the requirement as written
    - **Local Legal Conflict**: When a local law or regulation that applies to the supplier conflicts with the requirement as written.
    - **Contractual Conflict**: When conflicting language is present in the Microsoft contract with the supplier. If no language exists within the Microsoft/Supplier contract, this response should NOT be used.
    - **Does Not Apply** – With SSPA's recent update on requirement assignment, if your supplier receives a requirement, it likely applies to their services, or to the compliance level they have chosen within their profile.
    - **Not Compliant** – If the supplier has indicated compliance with the requirement and your findings are contrary.
    - **Partially Compliant** – If the supplier has indicated compliance with the requirement and your findings indicate they are only partially compliant.

    NOTE: The use of any response other than "Compliant", will need further verification from our SSPA support team. Please expect delays with the SSPA review when using these options.
6. **In the Assessor Remarks Column**: Include any additional information, including how this requirement was reviewed. Note: If your responses indicate local or contractual conflicts, specify the conflicting language from the supplier's contract with Microsoft or the relevant law/regulation. For 'Does Not Apply', "Not or Partially Compliant" responses, provide supporting details. Blanket responses like 'supplier doesn't process personal data' are not acceptable. SSPA requires specific comments related to the requirement. For example, for mobile device usage, if the response is 'Does Not Apply', specify that 'this supplier is not using mobile devices to process Microsoft data'.
7. **Initial the Acknowledgement Box**: Attest that the above responses are true and accurate to the best of your knowledge.
8. **Complete the Assessor Section:** Enter the assessor's details, sign and date the document, and confirm the supplier's compliance with Microsoft's Data Protection Requirements (DPR).
    - **Certification Number**: Provide the certification number or credential ID that qualifies you to perform the SSPA Independent Assessment. This should align with a recognized certification or affiliation (e.g., AICPA, IFAC, IAPP, ISACA), as outlined in the SSPA Program Guide. The certification may belong to either the individual assessor or the firm.
9. **Provide the completed document to the Supplier**: If you haven't already done so, remove the instructions and provide the table on letterhead to the supplier. They should then submit the assessment through the Microsoft Supplier Compliance Portal.

Independent Assessment for v10 DPR

Supplier Name:	*Name*		
Supplier number(s):	*Number* | *Number* | *Number*		

#	Requirement	Supplier Response	Assessor Response	Assessor Remarks and/or Procedural Info
Section A: Management				
1	Contract Language	Compliance Status	Compliance Status	
2	Subprocessor Agreements	Compliance Status	Compliance Status	
3	DPR Accountability	Compliance Status	Compliance Status	
4	Annual privacy & security training	Compliance Status	Compliance Status	
5	Sanctions	Compliance Status	Compliance Status	
6	Process Microsoft Personal Data as documented by Microsoft	Compliance Status	Compliance Status	
Section B: Notice				
7	Microsoft Privacy Statement	Compliance Status	Compliance Status	
8	Collecting Via Live or Recorded calls	Compliance Status	Compliance Status	
Section C: Choice and Consent				
9	Data Subject Consent	Compliance Status	Compliance Status	
10	Use of Cookies	Compliance Status	Compliance Status	
Section D: Collection				
11	Monitor the collection of data	Compliance Status	Compliance Status	
12	Collecting data from children	Compliance Status	Compliance Status	
13	Data set with reduced identifiability	Compliance Status	Compliance Status	
Section E: Retention				
14	Retention	Compliance Status	Compliance Status	
15	Return or Destroy (per Microsoft)	Compliance Status	Compliance Status	
Section F: Data Subjects				
16	Assist Microsoft w/ Data subject requests	Compliance Status	Compliance Status	

17	Data Subject identification	Compliance Status	Compliance Status	
18	Locate Personal Data (per Microsoft)	Compliance Status	Compliance Status	
19	Exercise Data Subject rights	Compliance Status	Compliance Status	
20	Record Data Subject requests	Compliance Status	Compliance Status	
21	Provide Personal data records	Compliance Status	Compliance Status	
22	Not able to identify anyone else	Compliance Status	Compliance Status	
23	Escalate complaints to Microsoft	Compliance Status	Compliance Status	
24	Track the recipients of shared data	Compliance Status	Compliance Status	
Section G: Subcontractors				
25	Notify of use or change in Subcontractors	Compliance Status	Compliance Status	
26	Document the nature and extent of Microsoft Personal and Confidential Data processed by Subcontractors	Compliance Status	Compliance Status	
27	Data Subject's stated contact preferences	Compliance Status	Compliance Status	
28	Limit data to what is necessary to fulfill the supplier's contract with Microsoft.	Compliance Status	Compliance Status	
29	Unauthorized or Unlawful Processing of Microsoft Personal Data	Compliance Status	Compliance Status	
30	Notify Microsoft of all unauthorized Processing	Compliance Status	Compliance Status	
31	Subcontractor collects Personal data from third parties	Compliance Status	Compliance Status	
32	Mitigate harm from unauthorized Processing	Compliance Status	Compliance Status	
Section H: Quality				
33	Data integrity	Compliance Status	Compliance Status	
Section I: Monitoring and Enforcement				
34	Incident Response & Notifications	Compliance Status	Compliance Status	
35	Incident Remediation Plan	Compliance Status	Compliance Status	
36	Data Protection Complaints	Compliance Status	Compliance Status	
Section J: Security				

37	Annual Security Assessments	Compliance Status	Compliance Status	
38	Mobile Device Policy	Compliance Status	Compliance Status	
39	Asset Inventory	Compliance Status	Compliance Status	
40	Access Rights Management Procedures	Compliance Status	Compliance Status	
41	Patch Management Procedures	Compliance Status	Compliance Status	
42	Anti-Virus and Anti-Malware	Compliance Status	Compliance Status	
43	Developing Software for Microsoft	Compliance Status	Compliance Status	
44	Data Loss Prevention	Compliance Status	Compliance Status	
45	Secrets in Software Development	Compliance Status	Compliance Status	
46	Backup Planning Processes	Compliance Status	Compliance Status	
47	Business Continuity Planning	Compliance Status	Compliance Status	
48	Authenticate Individuals	Compliance Status	Compliance Status	
49	Data in Transit Across Networks	Compliance Status	Compliance Status	
50	Disk Based Encryption	Compliance Status	Compliance Status	
51	Encryption at Rest	Compliance Status	Compliance Status	
52	Anonymize Personal Data	Compliance Status	Compliance Status	
Section K: AI Systems				
53	AI Systems contractual terms present in contract between Microsoft and Supplier	Compliance Status	Compliance Status	
54	Name the role of the person or group charged with ensuring compliance for AI Systems	Compliance Status	Compliance Status	
55	Annual Privacy and Security Training for AI System Data Handlers	Compliance Status	Compliance Status	
56	AI System Incident Response Plan	Compliance Status	Compliance Status	
57	Red Teaming and Vulnerability Mitigation	Compliance Status	Compliance Status	
58	Documented Responsible AI Program (Includes Requirements: 59-64)	Compliance Status	Compliance Status	
59	- Intended Uses Transparency Disclosures	Compliance Status	Compliance Status	

60	- Signed Agreements	Compliance Status	Compliance Status	
61	- Accountability	Compliance Status	Compliance Status	
62	- Risk Assessment	Compliance Status	Compliance Status	
63	- Transparency and Explainability	Compliance Status	Compliance Status	
64	- Monitoring and Adaptation	Compliance Status	Compliance Status	
65	Intended Use Reporting	Compliance Status	Compliance Status	
66	Updating (new or change) transparency disclosures and notifications to Microsoft	Compliance Status	Compliance Status	
67	Operating Procedure and Health Monitoring is in place	Compliance Status	Compliance Status	
68	Health Monitoring includes Methods Outlined	Compliance Status	Compliance Status	
69	Failure of Intended Use	Compliance Status	Compliance Status	
70	Biases and Discrimination Reporting	Compliance Status	Compliance Status	

Assessor's Acknowledgment of Accuracy and Supplier Compliance	
Assessor: Company Name	*Name*
Assessor: Name	*Name*
Assessor: Affiliation (see Program Guide)	*Certifying Body*
Assessor: Certification Number	*Number*
Assessor: Executive Statement	*Open Text Area (not required)*
Assessor: Procedural information	*Open Text Area (not required)*

By signing this document, I confirm that an accurate, independent assessment of the supplier's compliance with the Microsoft Data Protection Requirements (DPR) has been conducted, ensuring all relevant criteria have been thoroughly evaluated.

I acknowledge that:

- The supplier has provided all necessary disclosures, reporting, and documentation required for the assessment.
- The assessment has verified the supplier's compliance with the DPR.
- Any discrepancies or non-compliance issues identified during the assessment have been documented in the Assessor Remarks column and communicated to the supplier.
- At Microsoft's request, we will provide our internal testing documentation that supports the results of our assessment.

Assessor or Firm Signature	_____
Date (please use the specified format)	*MM/DD/YYYY*