Microsoft Procurement

Security & Privacy Assurance Program Guide

Version 5

November 2018

Introduction

At Microsoft, we believe that privacy is a fundamental right. In our mission to empower every individual and organization on the planet to achieve more, we strive to earn and maintain the trust of our customers every day.

Strong privacy and security practices are critical to our mission, essential to customer trust, and in several jurisdictions required by law. The standards captured in Microsoft's privacy and security policies reflect our values as a Company and these extend to our suppliers that process Microsoft data on our behalf.

The Supplier Security and Privacy Assurance ("SSPA") Program is Microsoft's corporate program in place to deliver Microsoft's data processing instructions to our Suppliers, in the form of the Microsoft Supplier Data Protection Requirements ("DPR"), downloadable from this webpage. The SSPA drives compliance to these requirements through an annual compliance cycle.

Definitions

"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.

"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.

"Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal 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.

An "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.

"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.

"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.

SSPA Program Overview and Scope

Processing Personal or Confidential Data on Microsoft's behalf means doing so as part of your performance per the terms of your purchase order or contract with Microsoft.

The SSPA program is a partnership between Microsoft Procurement, Corporate External and Legal Affairs, and Corporate Security to ensure that privacy and security principles are followed when suppliers Process Microsoft Personal Data and/or Microsoft Confidential Data.

The scope of the SSPA program covers all suppliers globally that Process Microsoft Personal and/or Confidential Data. Your Microsoft business owner(s) will determine whether engagements with your company require SSPA management.

The SSPA program requirements are outlined in the DPR. An annual self-attestation of compliance to these standards is required. Suppliers may also be selected to provide independent verification of compliance.

Important Note: Interactions with SSPA compliance activity determines a SSPA status of Green (complaint) or Red (non-compliant). Microsoft purchasing tools validate that the SSPA status is Green (for each supplier within scope for the SSPA program) prior to allowing an engagement to move forward. This applies to companies that are in-scope for SSPA management.

SSPA Annual Process Steps Diagram

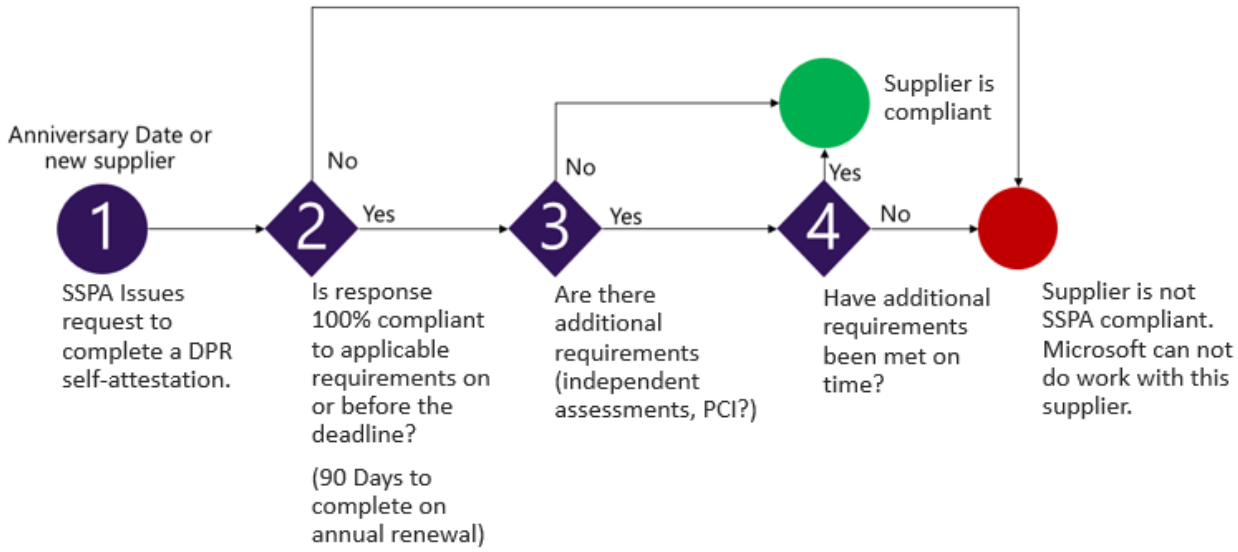

Table 1: Microsoft Personal Data in-scope for SSPA Compliance:

Data Type	Examples include but not limited to…
Sensitive Data	Data related to children Genetic data Biometric data Health data Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership A natural person's sex life or sexual orientation Immigration status (visa; work authorization etc) Government Identifiers (passport; driver's license; visa; social security numbers; national identify numbers) Precise user location data (within 300 meters)
Customer Content Data	Documents, photos, videos, music etc Reviews and/or ratings entered in a product or service Survey responses Browsing history, interests and favorites Inking, typing and speech utterance (voice/audio and/or chat/bot) Credential data (passwords, password hints, username, biometric data used for identification) Customer data associated with a support case
Captured and Generated Data	Imprecise location data IP address Device preferences and personalization Service usage for websites, webpage click tracking Social media data, social graph relationships Activity data from connected devices such as fitness monitors Contact data such as name, address, phone number, email address, date of birth, dependent and emergency contacts Fraud and risk assessment, background check Insurance, pension, benefit detail Candidate resumes, interview notes/feedback

Account Data	Payment instrument data Credit card number and expiration date Bank routing information Bank account number Credit requests Line of credit Tax documents and identifiers Investment data Corporate cards Expense data

Table 2: Microsoft Confidential/Highly Confidential Data in-scope for SSPA Compliance

Examples include but not limited to…	
Develop, test, or manufacture Microsoft Products or components of Microsoft Products. Microsoft software or hardware sold commercially in any channel is considered "Microsoft Product."	Highly Confidential
Device pre-release marketing information	Highly Confidential
Unannounced Microsoft corporate financial data subject to SEC rules.	Highly Confidential
Microsoft product license keys on behalf of Microsoft for distribution via any method.	Confidential
Develop or test Microsoft internal Line of Business (LOB) applications.	Confidential
Microsoft pre-release marketing material for Microsoft software and services such as Office, SQL, Azure, etc.	Confidential
Write, design, edit or print documentation for Microsoft services or devices (process or procedure guides, configuration data, etc.)?	Confidential
A Microsoft business owner may require participation for other data processing not included in this guide.	

Supplier Data Processing Profile

SSPA requires that your company completes a short profile to support compliance activity. The SSPA team, on information from the business, may update certain profile fields to trigger compliance activity.

For example, if your company does not disclose that you Process credit cards on Microsoft's behalf but the SSPA learns that this is the case, we will set the Payment Card Industry (PCI) flag to *yes* and your company will receive a request to provide a PCI certificate.

Your company can contact the SSPA team to verify the applicability of the activities issued by the program.

Self-Attestation Requirement

All SSPA enrolled suppliers are required to submit a self-attestation of compliance to the DPR within 90 days of receiving the request. This is an annual requirement. New suppliers enrolled in the SSPA program are required to complete this activity before a SSPA Status of Green (compliant) is secured.

An attestation update may be required mid-cycle where a new engagement indicates a change to the nature of Personal Data and/or Processing.

Your company SSPA Status will turn to RED (non-compliant) if the 90-day period is exceeded. The SSPA team is not authorized to provide extensions for DPR self-attestations.

New purchase orders cannot process until your SSPA Status turns to Green (compliant).

The Authorized Representative (see definition), is to

1. determine which requirements apply,
2. post a response to each applicable requirement, and
3. sign and submit the attestation in the Supplier Compliance Portal.

Applicability

Your company is expected to respond to all *applicable* DPR requirements. Some of the requirements may not apply to the goods or services your company provides to Microsoft.

In the event the Microsoft supplier operates as a Controller, with respect to the 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 the 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.

If you are unsure about which requirements apply, you can contact the SSPA team.

Your DPR submission will be reviewed by the SSPA team, who will check that the engagement activity associated to your supplier account supports your selections of 'applies' and 'does not apply' against each requirement. The team may request clarification before accepting the submission.

The SSPA team will ensure that local and contract conflict selections and associated comments include the relevant clauses that support the assertion.

Note: A selection of suppliers will also be asked to conduct an independent assessment (*See below*.)

Independent Assessment Requirement

The SSPA program will require independent verification of DPR compliance from suppliers considered high risk due to the nature of the data Processed.

Companies that meet the criteria are asked to select an independent auditor to assess compliance against the DPR, the assessor is to provide an unqualified letter of attestation to the SSPA.

Here is an outline of how to approach this requirement:

1. The engagement must be performed by an assessor with sufficient technical training and subject knowledge to adequately assess compliance.
2. Assessors must be affiliated with the International Federation of Accountants (IFAC) or the American Institute of Certified Public Accountants (AICPA), or must possess certifications from other relevant privacy and security organizations, such as the International Association of Privacy Professionals (IAPP) or the Information Systems Audit and Control Association (ISACA).
3. The assessor must use the most current DPR which includes the Evidence Required to support each requirement. You will need to provide your DPR attestation to the assessor.
4. In the case of a newly enrolled supplier, the assessor will test the design of the process controls. In all other cases, the auditor will test both the design of the process controls and the effectiveness of the controls.
5. The scope of the assessment engagement is limited to Microsoft Personal and/or Confidential Data Processed (e.g., collected, used, retained, or disclosed) as part of the performance per the terms of the supplier's purchase order, contract or statement of work with Microsoft.
6. The scope of the engagement is limited to those business segments and/or geographic locations that Process the Microsoft Personal and/or Confidential Data. The letter of attestation must include the list of locations included in the assessment.
7. The document submitted by the supplier to SSPA program must take the form of an unqualified letter of attestation. (See the sample letter in the Appendix).

SSPA can provide a list of preferred assessors on request. Suppliers are expected to pay for this assessment; the costs will vary depending on the scale and scope of the in-scope data processing.

Note: If your company has a security industry certification, it may be used as a substitute for the security requirements in the DPR, reducing the scope and therefore the cost of this independent assessment. (*See "Industry Certifications" section below*)

Independent Assessment Selection

The SSPA program collects information about the data associated to each in-scope supplier engagement at the time of purchasing. This informs the selection of companies to provide independent assurance of compliance.

A supplier will not be selected to conduct an independent assessment if all in-scope Microsoft data is Processed within the Microsoft network environment (with corporate credentials) or if the estimated volume of in-scope personal data records in a given year is less than 500.

A supplier will be selected to conduct an audit if any of the following attributes are true:

Data class = Highly Confidential

Microsoft Procurement managed supplier

Automated data subject rights obligation*

Cloud service (e.g., software as a service or "SaaS")

Website hosting services

Use of subcontractors to Process Microsoft Personal/Confidential Data.

*Microsoft division privacy teams make this determination

Industry Certifications

As an operating principle, SSPA allows industry certifications where they provide coverage for the standards contained in the DPR. Microsoft has incorporated the EU General Data Protection Regulation (GDPR) into our company privacy standard; this limits the certifications we can allow at this time.

Companies will be able to provide industry certifications to satisfy the *security* requirements in the DPR.

Table 3: Acceptable Independent Assessment Submissions

Scenario	Options
Personal Data only	Independent assessment based on all applicable portions of the DPR*
Confidential Data only	Independent assessment based on all applicable portions of the DPR *OR* SOC 2 type 2 report that includes security coverage *OR* ISO 27001 certification
Personal and Confidential Data	Independent assessment based on all applicable portions of the DPR OR Independent assessment based on the DPR [on all applicable portions other than the security sections] *AND* an ISO 27001 certification *OR* SOC 2 type 2 report with security coverage

* As certifications become available these options will expand.

PCI DSS Certification Requirement

The PCI Data Security Standard (PCI DSS) is a framework for developing a robust payment card data security process that includes prevention, detection and appropriate reaction to security incidents. The framework was developed by the PCI Security Standards Council, a self-regulatory industry organization. The purpose of the PCI DSS requirements is to identify technology and process vulnerabilities that pose risks to the security of cardholder data that is Processed.

Microsoft is required to comply with these standards. If you handle payment card information on our behalf we require evidence of your adherence to these standards. Consult the PCI Security standards council to understand the requirements set by the PCI organization.

Depending on the volume of transactions processed you will either be required to have an independent assessor certify compliance or you can complete a self-assessment. The forms are located here.

Payment card brands set the thresholds for assessment type:

- Level 1: Provide a 3rd Party Assessor PCI DSS certificate
- Level 2 or 3: Provide a PCI DSS Self-Assessment Questionnaire (SAQ) signed by a company officer.

The SSPA program accepts both types of assessments we ask that you submit the certification that applies and meets PCI requirements.

Supplementary Requirements

There are scenarios where Microsoft business groups require additional risk management activity. Your company may be selected for enrollment in supplementary requirements in addition to the SSPA process described above.

Supplementary requirements focus on information gathering and are not included in SSPA compliance verification.

Data Handling Incidents

Should a privacy or security incident occur, suppliers must inform Microsoft as detailed in the DPR.

You can e-mail SupplR@microsoft.com or use the SSPA Supplier Compliance Portal, in each case you will be asked to complete a short in-take form.

Appendix

On completion of an independent assessment, the assessor can prepare an unqualified letter of attestation based on the sample outline below. This is intended as a guide.

<Auditing company letterhead>

Date

Supplier Name

Supplier Address

Location assessed (append if multiple locations).

We have examined the design of _____ (the "Company") controls as of _____<assessment date>, over Microsoft Personal Data and/or Microsoft Confidential Data as defined in and in connection with the applicable sections and requirements of the Microsoft Supplier Data Protection Requirements (DPR), version __, to provide reasonable assurance t

The Company's management is responsible for the adequate design of these controls and compliance with the DPR. Our responsibility is to express an opinion on the hat the controls were designed in conformity with the DPR and that the design of these controls complies with the DPR. design of these controls and the Company's compliance based on our examination.

Our examination included (1) obtaining an understanding of the design of the Company's controls over the privacy and security of Microsoft Personal Data and Microsoft Confidential Data; and (2) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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

In our opinion, as of _____ <date> the Company in all material respects has adequately designed controls over the Microsoft Personal Data and/or Microsoft Confidential Data in its possession to provide reasonable assurance that this data is managed in conformity with the DPR.

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

Signature of Auditor

Auditor Name and Title