Crowe

Crowe as independent assessor

Supplier Security and Privacy Assurance (SSPA)

Audit / Tax / Advisory / Risk / IT

SSPA

Have you been acquainted with the term SSPA (Supplier Security & Privacy Assurance)?

Strong privacy and security practices are the key in today’s information-based economy. Such practices are required by law.

The Supplier Security and Privacy Assurance (SSPA) is a corporate program of the Microsoft corporation through which it delivers to its suppliers instructions for secure data processing in the form of “Microsoft Supplier Data Protection Requirements ” (DPR).

What is an SSPA Preferred Assessor?

A Preferred Assessor is a company that has been approved by Microsoft's procurement department to perform an independent assessment against Microsoft's Data Protection Requirements.

These companies understand the Microsoft SSPA program and are qualified to perform an SSPA assessment.

Scope – Data involved

Microsoft's in-house developed Supplier Security and Privacy Assurance (SSPA) program is an annual requirement once you become an active Microsoft supplier. The scope of the SSPA covers all suppliers globally that process Personal Data and/or Microsoft Confidential Data in connection with any active Master Service Agreement (MSA), Statement of Work (SOW) or Purchase Order (PO).

Basic goal

Microsoft Supplier Data Protection Requirements (“DPR”) apply to all suppliers to the Microsoft Corporation who process Microsoft’s personal and/or confidential data related to the service a supplier has contracted with the Microsoft Corporation.

Depending on the type of service which supplier is providing to the Microsoft Corporation and the type and confidentiality of data processed, a supplier is required to perform annual Self-attestation of compliance to the DPR.

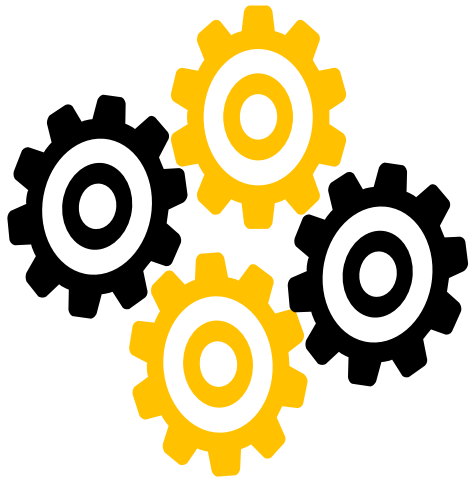
However, if the supplier is processing data which is considered personal and/or confidential according to Microsoft classification, he is obligated to render services of independent assessor for the „Independent assurance of compliance“ to the DPR. An evidence to performed independent assurance is the „Independent Assessment Letter“ issued by the assessor, and submitted to the Microsoft SSPA team by the supplier.

Data Protection

The DPR is made up of 10 categories that follow a Data Governance lifecycle model.

10 Categories are:

01 Management
02 Data Subjects
03 Notice
04 Disclosures to third parties
05 Choice and consent
06 Quality Start2021!
07 Collection
08 Monitoring and enforcement
09 Retention
10 Security



Applicability

One of the first steps in your Microsoft Supplier Security and Privacy Assurance (SSPA) journey is to correctly submit your Data Protection Requirements (DPR) “SSPA Applicability” self-assessment.

It is essential to align your “SSPA Applicability” profile with the service you are providing to Microsoft. Applicability relates to the type or types of data being processed, transmitted or exchanged.

Personal Data Examples:

01 Sensitive data 
02 Customer content data 
03 Capture and generate data 
04 Account data 

The key to any supplier compliance program is defining what information is needed and being collected. Microsoft’s SSPA requires you to establish your “Applicability” and then have it independently assessed against their Data Protection Requirements (DPR).

What can we do for you

Independent assurance of compliance

Crowe RS has the qualifications required by the Microsoft SSPA guide related to required expertise and sufficient technical training and subject knowledge to adequately assess compliance. Crowe RS is performing services of independent assessor and can assist you to fulfil annual requirements of the SSPA program.

01 Completed an Independent Assessment against the DPR;
02 Issuing SOC 2 (type 1 and type 2) reports;
03 Issuing Management Letter with detected discrepancies and advice on how to resolve

Issued Independent Assessment Letter