Microsoft Procurement

Supplier Security & Privacy Assurance (SSPA) Program Guide

Version 9

October 2023

Table of Contents

Introduction

At Microsoft, we believe 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 (such as your company) 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 baseline data processing instructions to our suppliers, in the form of the Microsoft Supplier Data Protection Requirements ("**DPR**"), available on the SSPA page on Microsoft.com/Procurement. Note that suppliers may have to meet additional organizational level requirements that are decided and communicated independently of SSPA by the Microsoft group responsible for the engagement with supplier.

Key SSPA terms are defined in the DPR. To learn more about the program, read our Frequently Asked Questions (FAQs) and engage our global team by writing to SSPAHelp@microsoft.com.

SSPA Program Overview

SSPA is a partnership between Microsoft Procurement, Corporate External and Legal Affairs, and Corporate Security to ensure privacy and security principles are followed by our suppliers.

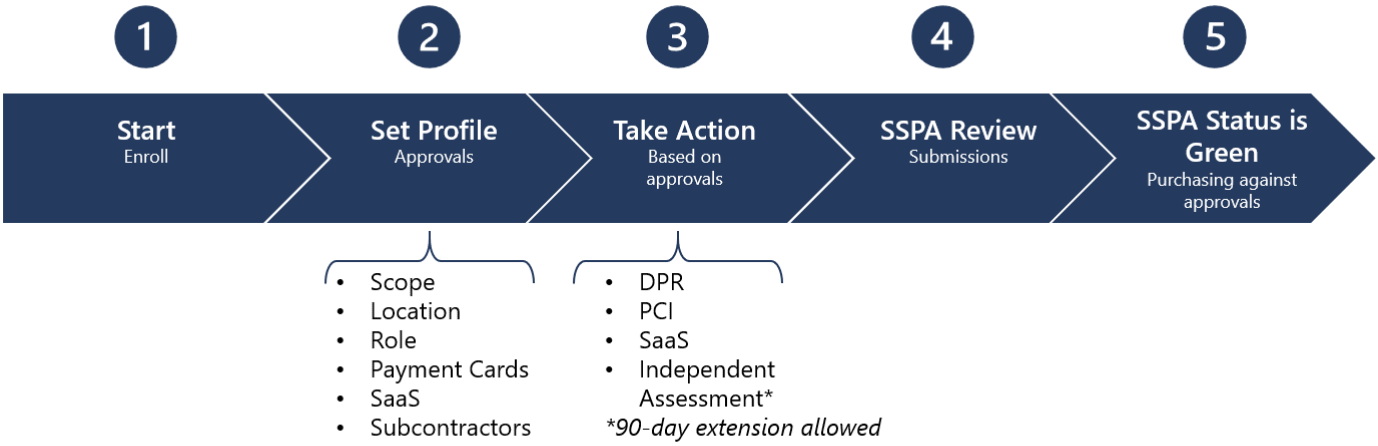
SSPA is a global program that covers suppliers that Process Personal Data and/or Microsoft Confidential Data in connection with that supplier's performance (e.g., provision of services, software licenses, cloud services), under the terms of its contract with Microsoft (e.g., Purchase Order terms, master agreement) ("**Perform,**" "**Performing**" or "**Performance**").

Suppliers are enabled to make Data Processing Profile selections that align to the goods and/or services you are contracted to Perform. These selections trigger corresponding requirements to provide compliance assurances to Microsoft.

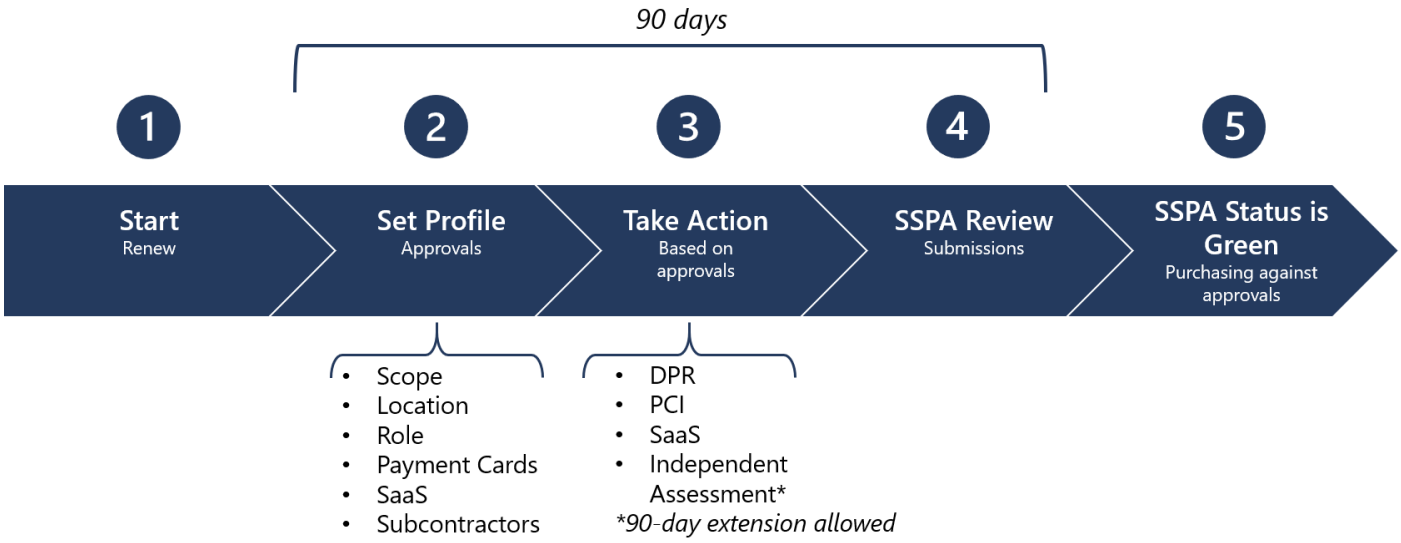
All enrolled suppliers will complete a self-attestation of compliance to the DPR annually. Your Data Processing Profile determines whether the full DPR is issued or if a subset of requirements applies. Suppliers that process what Microsoft considers higher risk data may also need to meet additional requirements, such as providing independent verification of compliance (see Independent Assessment). Suppliers that are on a published Microsoft Subprocessor list will also be asked to provide independent verification of compliance.

Important: Compliance activities determine an SSPA status of Green (compliant) or Red (non-compliant). Microsoft purchasing tools validate the SSPA status is Green (for each supplier in scope for SSPA) prior to allowing an engagement to move forward.

SSPA Process Diagram – New Supplier Enrollment



SSPA Process Diagram – Annual Supplier Renewal



SSPA Scope

To help determine whether you (the supplier) Process Personal Data and/or Microsoft Confidential Data, see the list of examples in the tables below. Please note that these are examples and not an exhaustive list.

Note: A Microsoft business owner may ask for an enrollment outside of this list considering the confidential nature of the data processed.

Personal Data by Data Type

Examples include but are not limited to:

Sensitive Data
Data related to children
Genetic, biometric, or health data
Racial or ethnic origin
Political, religious, or philosophical beliefs, opinions, and affiliations
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 identity numbers)
Precise user location data (within 300 meters)
Personal bank account numbers
Credit card number and expiration date; **or** security/access code or password/credentials allowing access to an account
End-user Pseudonymized Information (EUPI) (Identifiers created by Microsoft to identify users of Microsoft products and services) • Globally Unique Identifier (GUID) • Passport User ID or Unique Identifier (PUID) • Hashed End-User Identifiable Information (EUII) • Session IDs • Device IDs • Diagnostic data • Log data • 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
Metadata and telemetry
Account Data
Payment instrument data
Credit card number and expiration date
Bank routing information
Bank account number
Credit requests or line of credit
Tax documents and identifiers
Investment or expense data
Corporate cards
Online Customer Data
Microsoft online enterprise customer (Azure tenant, M365 tenant, etc.)
Microsoft consumer customer (Xbox Live, OneDrive Consumer)
Microsoft enterprise customer (on premises customer)
Support data (customer originates a ticket)
Account data (billing data, e-commerce)
Survey/event registration/training

Protected Health Information
National identification numbers (including tribal numbers and health information identification numbers)
Demographic data used in a Protected Health Information (PHI) context: • Birth date • Gender • Ethnicity • Biometric data • Full face photographs • Address (full or partial) • Contact information • Emergency contact data

Microsoft Confidential Data

Examples include but are not limited to:

Highly Confidential
Information concerning or related to the development, testing, or manufacturing of Microsoft Products or components of Microsoft Products *Microsoft software, online services, or hardware sold commercially in any channel is considered "**Microsoft Product**"* **Note:** For Gaming product development, the Microsoft business owner can indicate whether the work product should have a Data Classification of Highly Confidential or Confidential.
Microsoft device pre-release marketing information
Unannounced Microsoft corporate financial data subject to SEC rules
Confidential
Microsoft product license keys on behalf of Microsoft for distribution via any method
Information concerning or related to the development or testing of Microsoft internal Line of Business (LOB) applications
Microsoft pre-release marketing materials for Microsoft software and services such as Office, SQL, Azure, etc.
Written, design, electronic, or print documentation for any Microsoft services or products, such as devices (process or procedure guides, configuration data, etc.)

Important: A Microsoft business owner may require participation for data not included in this list.

Data Processing Profile

Microsoft suppliers have control over their SSPA Data Processing Profile.

This allows suppliers to decide which engagements they want to be eligible to Perform. Pay careful attention to the selections and consider the compliance activity that must be completed to achieve the approval. **See the "Assurance Requirements" Section below and Appendix A**.

Microsoft business groups will only be able to create engagements with suppliers where the data processing activity matches the approvals the supplier obtained.

Suppliers will be able to update their Data Processing Profile at any time during the year **if there are no open tasks**. When a change is made, the corresponding activity will be issued and must be completed before the approvals are secured. The existing, completed approvals will apply until newly issued requirements are completed.

If the newly executed tasks are not completed within the 90-day time frame allowed, the SSPA status will turn to Red (non-compliant), and the account is at risk of being deactivated from Microsoft Accounts Payable systems.

Data Processing Approvals	
1	Data Processing Scope ▪ Confidential ▪ Personal, Confidential
2	Data Processing Location ▪ At Microsoft or Customer ▪ At Supplier
3	Data Processing Role ▪ Controller ▪ Processor ▪ Subprocessor (designated by Microsoft)
4	Payment Card Processing ▪ Yes ▪ Not applicable
5	Software as a Service ▪ Yes ▪ Not applicable
6	Use of Subcontractors ▪ Yes ▪ Not applicable

Approval and Profile Considerations

Data Processing Scope

Confidential

Select this approval if the supplier's Performance will involve Processing of only Microsoft Confidential Data.

If you select this approval, you will not be eligible for Personal Data processing engagements.

Personal, Confidential

Select this approval if the supplier's Performance will involve Processing of Personal Data and Microsoft Confidential Data.

Processing Location

At Microsoft or Customer

Select this approval if supplier's Performance involves supplier's Processing of data within the Microsoft network environment where staff use *@microsoft.com* access credentials or within the environment of a Microsoft customer.

Do not select this option under these circumstances:

- Supplier manages a Microsoft designated offshore facility (OF).
- Supplier provides resources to Microsoft, and they work on and off the Microsoft network at times. The processing location for working off-network is considered "at supplier."

At Supplier

If the condition "At Microsoft or Customer" (as described above) does not apply, select this option.

Data Processing Role

Controller

Select this approval if **all** aspects of Performance by supplier meet the Controller data processing role definition (see DPR).

If you select this approval, you will not be eligible for Personal Data processing with the 'Processor' role designation. If supplier is both a Processor and a Controller to Microsoft, do not select 'Controller', select Processor.

Processor

This is the most common processing role when suppliers Process data on behalf of Microsoft. Please review the definition of Processor in the DPR.

Subprocessor

Suppliers cannot self-identify as a Subprocessor at Microsoft because it requires pre-approval by internal Privacy teams. Please review the definition of Subprocessor in the DPR. Subprocessors will have additional contract and compliance requirements, including a Data Protection Addendum and an Independent Assessment (see below).

Payment Card Processing

Select this approval if any part of the data Processed by supplier includes data to support credit card or other payment card processing on behalf of Microsoft.

This approval allows a supplier to engage in payment card processing engagements.

Software as a Service (SaaS)

Software as a Service (SaaS) allows users to connect to and use cloud-based applications over the Internet. For SSPA compliance purposes, view SaaS broadly to also include platform as a service (PaaS), and infrastructure as a service (IaaS). (To learn more about SaaS please see this explanation.)

Microsoft defines **Software as a Service (SaaS)** as software based on common code used in a one-to-many model on a pay-for-use basis or as a subscription based on use metrics. The cloud service provider develops and maintains cloud-based software, provides automatic software updates, and makes software available to its customers via the internet on a one-to-many, pay-as-you-go basis. This method of software delivery and licensing allows software to be accessed online via a subscription rather than bought and installed on each individual computer.

Note: Most SaaS suppliers will need to add the Subcontractor approval in the Microsoft Supplier Compliance Portal if the Personal Data or Microsoft Confidential data is hosted on a 3rd party platform or cloud infrastructure provider.

Website Hosting

Select this profile option if supplier hosts websites on Microsoft's behalf (see DPR for definition).

Use of Subcontractors

Select this approval if supplier uses Subcontractors to Perform (see DPR for definitions).

This also includes Freelancers (see DPR).

Healthcare

Select this profile option if supplier is required to process Protected Health Information (see DPR for definitions).

Assurance Requirements

Requirements based on Profile Approvals

The approvals selected in your Data Processing Profile assists SSPA in assessing the risk level across your Microsoft's engagement(s). SSPA compliance requirements differ based on the Data Processing Profile and associated approvals. This section explains the different SSPA requirements.

There are also combinations that may elevate or reduce compliance requirements. The combinations are captured in Appendix A and this is what you can expect to execute from the Microsoft Supplier Compliance Portal upon completing your profile. You can always validate how your scenario fits into this framework by requesting an SSPA team review.

Action: Find your approval profile in Appendix A and review the corresponding assurance requirements and Independent Assurance options, if applicable.

Important: If your profile includes Software as a Service (SaaS), Subcontractors, website hosting, or payment cards additional assurance is required.

Self-Attestation to the DPR

All suppliers enrolled in SSPA must complete a self-attestation of compliance to the DPR within 90 days of receiving the request. This request will be provided on an annual basis but may be more frequent if the Data Processing Profile is updated mid-year. Supplier accounts will change to an SSPA status of Red (non-compliant) if the 90-day period is exceeded. New in-scope purchase orders cannot be processed until the SSPA status turns to Green (compliant).

Newly enrolled suppliers must complete issued requirements to secure a SSPA status of Green (compliant) before engagements can begin.

Important: The SSPA team is not authorized to provide extensions for this task.

Suppliers are expected to respond to all applicable DPR requirements issued per the Data Processing Profile. It is expected that, within the issued requirements, a few may not apply to the goods or services the supplier provides to Microsoft. These can be marked as 'does not apply' with a detailed comment for SSPA reviewers to validate.

DPR submissions are reviewed by the SSPA team for any selections of 'does not apply', 'local legal conflict' or 'contractual conflict' against issued requirements. The SSPA team may ask for clarification of one or more selections. Local legal and contract conflicts are only accepted if supporting references are provided and the conflict is clear.

Authorized representatives that will complete the self-attestation should ensure they have sufficient information from subject matter experts to reply to each requirement with confidence. In addition, by adding their name to a SSPA form they are certifying that they have read and understand the DPR. Suppliers can add other contacts to the online tool to assist with completing the requirements.

The Authorized Representative (see DPR for definition), is to:

1. Determine which requirements apply.
2. Post a response to each applicable requirement.
3. Sign and submit the attestation in the Microsoft Supplier Compliance Portal.

Note: SSPA may ask for collaborating evidence of compliance for a particular Data Protection Requirement to support compliant attestations.

Independent Assessment Requirement

Please see the Requirements by Approvals in Appendix A to see the data processing approvals that trigger this requirement.

Suppliers have the option to change approvals by updating their Data Processing Profile. However, if the supplier has a Data Processing Role of "Subprocessor", the supplier cannot change this approval and will be required to have an Independent Assessment conducted annually.

To secure the approvals that require independent verification of compliance, suppliers will need to select an independent assessor to validate compliance against the DPR. The assessor is to prepare an advisory letter to provide compliance assurances to Microsoft. This letter must be unqualified and all non-compliant issues must be resolved and remediated before the confirmation letter is submitted to the Microsoft Supplier Compliance Portal for SSPA team review. Assessors can download an approved advisory letter template, which is attached to the "Preferred Assessors" PDF available here.

Appendix A includes acceptable certification alternatives if you elect not to use an independent assessor to verify compliance to the DPR (when applicable, such as for SaaS suppliers, website hosting suppliers or suppliers with Subcontractors). The ISO 27701 (privacy) and ISO 27001 (security) are relied on as providing close mapping to the DPR.

Where Supplier is a covered entity or healthcare service provider in the United States, we will accept a HITRUST report for privacy and security coverage.

If circumstances beyond standard triggers warrant additional due diligence, SSPA may require an independent assessment regardless of the Data Processing Profile. Examples include a request from division privacy or security; validation of data incident remediation; or requirement for automated data subject rights execution.

Guidance on 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. **Suppliers will need to provide their most recently approved DPR attestation responses 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 assessor will test the effectiveness of the controls.
5. The scope of the assessment engagement is limited to Personal Data and/or Microsoft Confidential Data in connection with that supplier's Performance.
6. 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 more than one supplier account at one time, the **letter of attestation must include the list of supplier accounts included in the assessment and associated addresses.**
7. 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.

SSPA has made a list of preferred assessors available. These companies are familiar with conducting SSPA assessments. Suppliers are expected to pay for this assessment; the costs will vary depending on the scale and scope of the data processing.

PCI DSS Certification Requirement

The Payment Card Industry Data Security Standard (PCI DSS) is a framework for developing robust payment card data security 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 a supplier handles payment card information on Microsoft's behalf, we require evidence of 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, a supplier will either be required to have a Qualified Security Assessor certify compliance or can complete a self-assessment questionnaire form.

Payment card brands set the thresholds for assessment type, typically:

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

Submit the certification that applies and meets PCI requirements. Suppliers who process or store Microsoft customer payment data must possess a current PCI Tier 1 certification as a service provider.

Software as a Service Requirement

Suppliers that meet the SaaS definition included on the Data Processing Profile may be required to provide a valid ISO 27001 certification if this is required in the Microsoft Cloud Services Agreement.

SSPA reviewers will validate that your submission meets the contract obligation.

Please do not submit a datacenter certification. We expect the ISO 27001 certification that applies to the software service(s) noted in your contract with Microsoft.

Use of Subcontractors

Microsoft considers the use of subcontractors a high-risk factor. Suppliers using subcontractors who will Process Personal and or Microsoft Confidential Data must disclose those subcontractors. Additionally, the supplier should also disclose the countries where that personal data will be processed by each subcontractor.

Data Incidents

If a supplier becomes aware of a privacy or security data incident, suppliers must inform Microsoft as detailed and defined in the DPR.

Report a data incident using SupplierWeb or email SuppIR@microsoft.com.

Be sure to include:

- Data incident date
- Supplier name
- Supplier number
- Microsoft contact(s) notified
- Associated PO, if applicable/available
- Summary of the data incident.

Appendix A

Requirements based on Profile Approvals

#	Profile	Assurance Requirements	Independent Assurance Options
1	**Scope**: Personal, Confidential **Processing Location:** At Microsoft or Customer **Processing Role:** Processor or Controller **Data Class:** Confidential or Highly Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR	
2	**Scope:** Confidential **Processing Location:** At Supplier **Processing Role:** N/A **Data Class:** Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR	
3	**Scope**: Confidential **Processing Location:** At Supplier **Processing Role:** N/A **Data Class:** Highly Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete an Independent Assessment against the DPR, **or** 2. Submit ISO 27001

#	Profile	Assurance Requirements	Independent Assurance Options
4	**Scope:** Personal, Confidential **Processing Location:** At Supplier **Processing Role:** Processor **Data Class:** Highly Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete an Independent Assessment against the DPR, 2. Independent Assessment against sections A-I of the DPR and ISO 27001, **or** 3. Submit ISO 27701 **and** ISO 27001
5	**Scope:** Personal, Confidential **Processing Location:** At Supplier **Processing Role:** Processor **Data Class:** Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR	
6	**Scope:** Personal, Confidential **Processing Location:** At Supplier **Processing Role:** Controller **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR	

#	Profile	Assurance Requirements	Independent Assurance Options
7	**Scope:** Personal, Confidential **Processing Location:** Any **Processing Role:** Subprocessor (This role is determined by Microsoft – profile will read "Subprocessor Approval: Yes") **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **SaaS:** N/A **Use of Subcontractors:** N/A **Website Hosting:** N/A **Healthcare:** N/A	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete Independent Assessment against the DPR, 2. Independent Assessment against sections A-I of the DPR and ISO 27001, **or** 3. Submit ISO 27701 **and** ISO 27001
Impact of adding SaaS, Subcontractors, Website Hosting, Healthcare			
8	**Scope:** Personal, Confidential **Processing Location:** At Supplier **Processing Role:** Processor **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **Subcontractors:** YES or **SaaS:** YES or **Website Hosting:** YES or **Healthcare:** YES	Self-attestation of compliance to the DPR **and** Independent Assurance of compliance	Independent Assurance options: 1. Complete Independent Assessment against the DPR, 2. Independent Assessment against sections A-I of the DPR and ISO 27001, **or** 3. Submit ISO 27701 **and** ISO 27001 **or** 4. HITRUST report (**only** for a covered entity or healthcare service provider in the US)

#	Profile	Assurance Requirements	Independent Assurance Options
9	**Scope:** Personal, Confidential **Processing Location:** At Supplier **Processing Role:** Controller **Data Class:** Highly Confidential or Confidential **Payment Cards:** N/A **Subcontractors:** YES or **SaaS:** YES or **Website Hosting:** YES or **Healthcare:** YES	Self-attestation of compliance to the DPR	
Additional assurance for Payment Cards and SaaS			
10	Any of the profiles above and **Payment Cards**	Above requirements that apply and Payment Card Industry assurance	Submit PCI DSS Certification
11	Any of the profiles above and **Software as a Service (SaaS)**	Above requirements that apply **and** submit your contractually required ISO 27001 certification covering the functional services.	Submit an ISO 27001 certification with functional coverage of the service(s) provided.