Microsoft Procurement

Guida al programma Garanzia di sicurezza e privacy dei fornitori (SSPA)

Versione 8

Giugno 2022

Introduzione

A Microsoft crediamo che la privacy sia un diritto basilare. Nella nostra missione, che consiste nel permettere a ogni persona e organizzazione del pianeta di ottenere di più, ci impegniamo ogni giorno per guadagnare e mantenere la fiducia dei nostri clienti.

Robuste pratiche di privacy e sicurezza sono critiche per la nostra missione, essenziali per la fiducia dei clienti e richieste per legge in molte giurisdizioni. Gli standard incorporati nelle politiche di Microsoft su privacy e sicurezza riflettono i nostri valori come azienda e si estendono anche ai fornitori (come la vostra compagnia) che trattano in dati di Microsoft per conto dell'azienda.

Il programma Supplier Security and Privacy Assurance ("**SSPA**") (Garanzia di sicurezza e privacy dei fornitori) rappresenta il programma aziendale di Microsoft instaurato per fornire ai fornitori di Microsoft le istruzioni dell'azienda per il trattamento dei dati sotto forma di Supplier Data Protection Requirements ("**DPR**") (Requisiti di protezione di dati dei fornitori) disponibile presso SSPA on Microsoft.com/Procurement. Notare che i fornitori potrebbero dover soddisfare requisiti supplementari a livello organizzativo che sono stabiliti e comunicati al di fuori di SSPA dal gruppo di Microsoft responsabile per l'incarico al fornitore.

I termini chiave SSPA sono definiti nel DPR. Per maggiori informazioni sul programma, vedere le Domande frequenti (FAQ) e rivolgersi al nostro team globale scrivendo a SSPAHelp@microsoft.com.

Panoramica del programma SSPA

SSPA è una partnership tra Microsoft Procurement, Corporate External e Legal Affairs e Corporate Security per garantire che i principi di privacy e sicurezza siano seguiti dai fornitori.

L'ambito di SSPA include tutti i fornitori in tutto il mondo che trattano dati personali e/o dati riservati di Microsoft in connessione con la prestazione del fornitore (ad esempio, fornitura di servizi, licenze di software, servizi cloud) in base ai termini del suo accordo con Microsoft (ad esempio, condizioni dell'ordine di acquisto, accordo quadro) (nel seguito "**Eseguire**", "**Esecuzione**" o "**Prestazione**")

SSPA consente al fornitore di selezionare profili di elaborazione dei dati che si allineano con i beni e/o servizi che il fornitore è stato incaricato di Eseguire. Queste selezioni attivano requisiti corrispondenti che forniscono a Microsoft garanzia di conformità.

Tutti i fornitori registrati dovranno compilare annualmente un'autocertificazione di conformità al DPR. Il profilo di elaborazione dati del fornitore stabilisce se viene emesso un DPR completo o se si applica solo un sottoinsieme dei requisiti. I fornitori che trattano dati che Microsoft considera ad alto rischio potrebbero anche dover soddisfare requisiti supplementari come una verifica di conformità fornita da parte indipendente. Anche ai fornitori elencati in elenchi pubblicati di sub-responsabili di Microsoft sarà richiesta la verifica di conformità fornita da parte indipendente.

Importante: le attività di conformità stabiliscono lo stato di SSPA, Verde (in conformità) o Rosso (non in conformità). Prima di consentire a un incarico di procedere, gli strumenti di acquisto di Microsoft convalidano che lo stato SSPA sia Verde (per ogni fornitore che rientra nell'ambito di SSPA).

Diagramma di processo SSPA – Iscrizione di fornitore nuovo

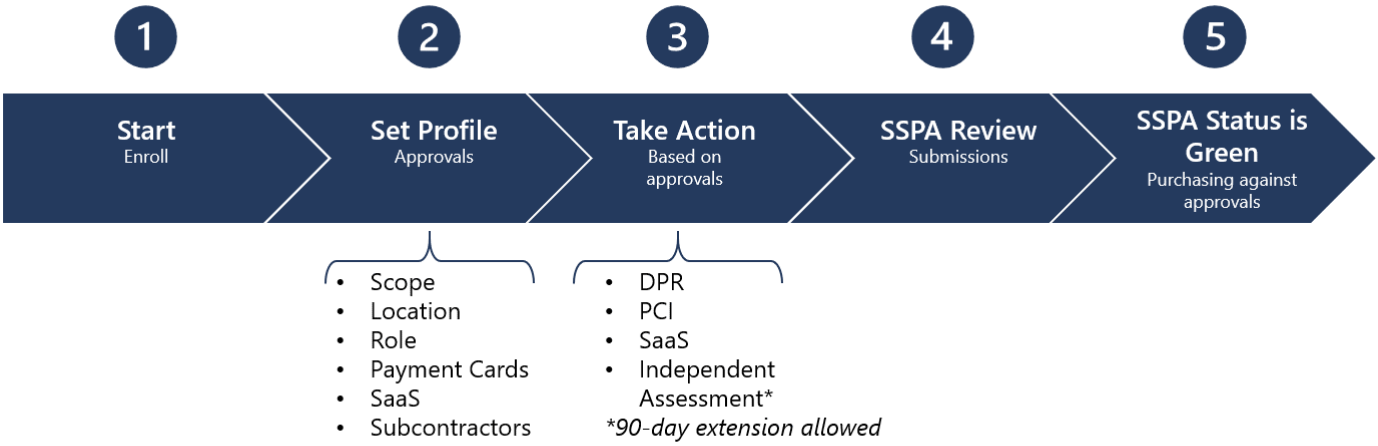
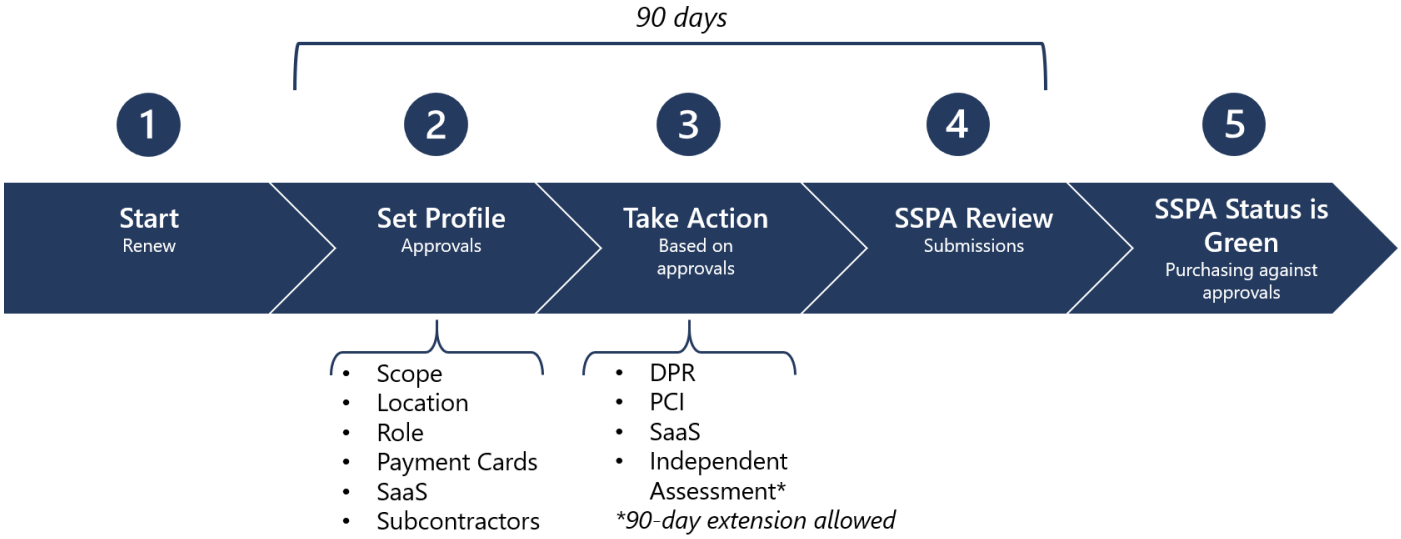


Diagramma di processo SSPA – Rinnovo annuale di fornitore



Ambito di SSPA

Per aiutarsi a stabilire se il fornitore tratta dati personali e/o dati riservati di Microsoft, vedere gli esempi elencati nella tabella sottostante. Notare che si tratta di elenco a scopo esemplificativo e non esaustivo.

Nota: considerata la natura riservata del dati trattati, i proprietari di attività Microsoft potranno richiedere l'iscrizione al di fuori dell'elenco.

Dati personali per tipo di dati

Esempi a scopo esemplificativo non esaustivo

Dati sensibili
Dati riguardanti i bambini
Dati genetici. Dati biometrici o dati sanitari
Origine razziale o etnica
Persuasione, opinione e appartenenza politica, religiosa o filosofica
Appartenenza sindacale
Vita o orientazione sessuale della persona
Stato di immigrazione (visto, permesso di lavoro, ecc.)
Documenti di riconoscimento (passaporto, patente di guida, visto, numeri di previdenza sociale, numeri d'identità nazionale)
Dati di posizione precisa dell'utente (entro 300 metri)
Numeri di conto bancario personale
Numero di carta di credito e data di scadenza
Dati sui contenuti dei clienti
Documenti, fotografie, video, musica, ecc.
Recensioni e/o valutazioni registrate di prodotto o servizio
Risposte a sondaggi
Cronologia di navigazione, interessi e preferiti
Inking, registrazione ed espressione vocale (video/audio e/o chat/bot)
Dati delle credenziali (password, suggerimenti di password, username, dati biometrici usati a scopo di riconoscimento)
Dati del cliente associati a una richiesta di assistenza

Dati acquisiti e generati
Dati di posizione imprecisa
Indirizzo IP
Preferenze e personalizzazione del dispositivo
Uso di servizio per siti web e monitoraggio dei clic in pagine web
Dati di social media, grafici e rapporti
Dati di attività da dispositivi collegati come dispositivi di controllo di fitness
Dati di contatto come nome, indirizzo, numero telefonico, indirizzo email, data di nascita, contatti di dipendente e emergenza
Frode e valutazione del rischio, controllo dei precedenti
Assicurazione, pensione, dettaglio dei benefici
Curriculum vitae del candidato, appunti/feedback di colloquio
Metadata and telemetry
Dati di account
Dati mezzo di pagamento
Numero di carta di credito e data di scadenza
Informazioni di coordinate bancarie
Numero di conto bancario
Domande di credito o linea di credito
Documenti e identificativi fiscali
Dati di investimenti e spese
Carte aziendali
Informazioni pseudonimizzate degli utenti (EUPI) (Identificativi creati da Microsoft per riconoscere gli utenti di prodotti e servizi di Microsoft)
Globally Unique Identifier (GUID) (Identificatore univoco globale)
Passport User ID o Unique Identifier (PUID) (ID utente del passaporto o identificatore univoco)
Hashed End-User Identifiable Information (EUII) (Informazioni hash identificazione utente)
ID sessione
ID dispositivo
Dati di diagnostica
Dati di log

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Dati riservati di Microsoft per classe di dati

Esempi a scopo esemplificativo non esaustivo

Altamente riservati
Informazioni riguardanti o relative allo sviluppo, collaudo o fabbricazione di prodotti Microsoft o componenti di prodotti Microsoft. *Il software di Microsoft, i servizi online o l'hardware venduto commercialmente in qualsiasi canale è considerato un "**Prodotto Microsoft**"*
Informazioni di marketing pre-release di dispositivi Microsoft
Dati finanziari aziendali di Microsoft soggetti alle norme SEC non ancora annunciati
Riservati
Chiavi di licenza Microsoft a nome di Microsoft per distribuzione in qualsiasi modo
Informazioni concernenti o relative allo sviluppo o collaudo di applicazioni Line of Business (LOB) (ramo di attività) interne di Microsoft
Materiali pre-release di Microsoft per software e servizi Microsoft come Office, SQL, Azure, ecc.
Documentazione scritta, di concezione, elettronica o stampata di qualsiasi servizio o prodotto Microsoft, come i dispositivi (guide di processo o procedurali, dati di configurazione, ecc.)

Importante: i proprietari di attività Microsoft potranno richiedere partecipazione per dati non inclusi in questo elenco.

Profilo trattamento dati

I fornitori di Microsoft possono controllare il loro profilo di trattamento dati SSPA.

In questo modo i fornitori possono decidere quali incarichi desiderano poter Eseguire. Prestare molta attenzione alla scelta e considerare l'attività di conformità che deve essere portata a termine per ottenere l'approvazione. **Vedere "Requisiti assicurativi" nella sezione sottostante e nell'appendice A**

I gruppi di business di Microsoft saranno in grado di creare incarichi solo per fornitori la cui attività di trattamento dati corrisponde all'approvazione da loro ottenuta.

I fornitori potranno aggiornare il Profilo trattamento dati in qualsiasi momento dell'anno **qualora non ci siano compiti aperti**. Quando viene effettuato un cambiamento, sarà emessa l'attività corrispondente che deve essere completata prima di potersi assicurare l'approvazione. L'approvazione in essere completata sarà applicata finché i nuovi requisiti emessi non siano stati portati a termine.

Se i nuovi compiti non sono portati a termine entro i 90 giorni ammessi, lo stato SSPA diventa Rosso (non in conformità) e l'account è posto a rischio di essere disattivato dai sistemi account fornitori di Microsoft.

Approvazione trattamento dati	
1	Ambito trattamento dati ▪ Riservati ▪ Personali, riservati
2	Sito trattamento dati ▪ Presso Microsoft o il cliente ▪ Presso il fornitore
3	Ruolo trattamento dati ▪ Revisore (indipendente o congiunto) ▪ Responsabile del trattamento ▪ Subappaltatore (designato da Microsoft)
4	Trattamento carte di pagamento ▪ Sì ▪ Non applicabile
5	Software come servizio ▪ Sì ▪ Non applicabile
6	Uso di subappaltatori ▪ Sì ▪ Non applicabile

Note sull'approvazione

Ambito trattamento dati

Riservati

Selezionare questa approvazione se la Prestazione del fornitore comporta solo il trattamento di dati riservati di Microsoft.

Se si sceglie questa approvazione non si sarà idonei a incarichi di trattamento di dati personali.

Personali, riservati

Selezionare questa approvazione se la Prestazione del fornitore comporta il trattamento di dati personali e dati riservati di Microsoft.

Sito trattamento dati

Presso Microsoft o il cliente

Selezionare questa approvazione se la Prestazione del fornitore comporta il trattamento dati del fornitore nell'ambiente della rete Microsoft in cui il personale usa credenziali di accesso *@microsoft.com* o nell'ambiente di un cliente di Microsoft.

Non selezionare questa opzione nelle seguenti circostanze:

- Il fornitore gestisce una struttura di Microsoft designata offshore (OF).
- Il fornitore procura le risorse a Microsoft e a volte opera di tanto la rete di Microsoft. Il sito di trattamento per operare fuori rete è considerato "presso il fornitore".

Presso il fornitore
Selezionare questa opzione se la condizione "Presso Microsoft o il cliente" (come descritta sopra) non si applica.

_____

Ruolo trattamento dati

Revisore (comprende indipendente e congiunto)

Selezionare questa approvazione se **tutti** gli aspetti della Prestazione da parte del fornitore soddisfano la definizione di revisore trattamento dati (vedere DPR).

Se si sceglie questa approvazione non si sarà idonei al trattamento di dati personali con il ruolo di 'Responsabile del trattamento'. Se il fornitore è sia un Responsabile del trattamento che un Revisore per Microsoft, non scegliere 'Revisore', ma scegliere Responsabile del trattamento.

Responsabile del trattamento

Questo è ruolo di trattamento più comune quando il fornitore tratta i dati per conto di Microsoft. Esaminare la definizione di Responsabile del trattamento in DPR.

Sub-responsabile del trattamento

Il sub-responsabile del trattamento è una terza parte che Microsoft impegna per l'Esecuzione quando la Prestazione include dati personali di Microsoft per i quali Microsoft è il Responsabile del trattamento. I fornitori non possono identificarsi come Sub-responsabili del trattamento di Microsoft perché ciò richiede l'approvazione a priori dei team di Privacy interni. I fornitori possono essere Sub-responsabili del trattamento quando Microsoft è il Responsabile del trattamento dati e il fornitore elabora tipi di dati personali aziendali idonei. I Sub-responsabili del trattamento avranno diversi requisiti di contratto e conformità, compresi un Addendum sulla protezione dei dati e una Valutazione indipendente (vedere sotto).

Trattamento carte di pagamento

Selezionare questa approvazione se una parte qualsiasi dei dati trattati dal fornitore include dati in supporto dell'elaborazione di carte di credito o altre carte di pagamento per conto di Microsoft.

Questa approvazione consente al fornitore di impegnarsi in incarichi di elaborazione delle carte di pagamento.

_____

Software

Microsoft Procurement guida gli acquirenti, per tutti gli acquisti di software, attraverso un processo di assunzione che include vari controlli, compreso il triage SSPA per decidere se il fornitore che procura il software rientra nell'ambito della gestione SSPA. (Per maggiori dettagli, gli acquirenti di Microsoft potranno riferirsi alle fasi delineate nella pagina interna Software ProcureWeb e servizio Cloud). Quando il programma SSPA è richiesto, i fornitori devono anche specificare che si applica il profilo 'Software come servizio' (SaaS). Per fornitori registrati nel programma SSPA, ciò può essere fatto al momento di compilare il Profilo trattamento dati nel Portale di conformità dei fornitori Microsoft.

Per finalità di conformità SSPA, SaaS può essere visto in linea di massima come comprendente anche Piattaforma come servizio (PaaS) e Infrastruttura come servizio (IaaS). (Per saperne di più su SaaS vedere questa spiegazione.)

Software come servizio(SaaS)

Software come servizio (SaaS) consente agli utenti di collegarsi e usare su Internet applicazioni basate su cloud.

Microsoft definisce Software come servizio (SaaS) il software basato su codice comune utilizzato in un modello uno a molti su base a consumo (pay-for-use) o come abbonamento basato su metriche di utilizzo. Il fornitore di servizio cloud sviluppa e cura la manutenzione di software basato su cloud, fornisce aggiornamenti di software automatici e rende disponibile il software ai suoi clienti tramite Internet come uno a molti, su base a consumo (pay-as-you-go). Questo metodo di fornitura e licenza del software rende il software accessibile online tramite abbonamento invece dell'acquisto e installazione su ogni individuale computer.

Nota: la maggioranza dei fornitori di SaaS deve aggiungere l'approvazione di un contratto di Subappaltatore nel portale di conformità dei fornitori Microsoft quando i dati personali o i dati riservati di Microsoft sono ospitati su una piattaforma di terza parte.

Uso di subappaltatori

Selezionare questa approvazione se il fornitore utilizza Subappaltatori per l'Esecuzione (vedere la definizione in DPR).

Ciò include anche i freelance (vedere DPR).

Requisiti di garanzia

Requisiti basati su approvazioni di profilo

Le approvazioni scelte nel proprio Profilo di trattamento dati aiutano il programma SSPA a valutare il livello di rischio nei confronti dell'impegno(i) con Microsoft. I requisiti di conformità SSPA sono diversi a seconda del Profilo trattamento dati e delle approvazioni ad esso associate. Questa sezione spiega i diversi requisiti di SSPA.

Ci sono anche combinazioni che possono aumentare o ridurre i requisiti di conformità. Le combinazioni sono illustrate nell'Appendice A e rappresentano ciò che ci si può aspettare nel portale di conformità dei fornitori Microsoft al momento della messa in atto dopo avere completato il profilo. Si può sempre verificare come il proprio scenario si adatti al framework richiedendo che il team SSPA lo esamini.

Azione: trovare il proprio profilo nell'Appendice A ed esaminare i corrispondenti requisiti di garanzia e, se applicabili, le opzioni di Garanzia indipendente.

Importante: è richiesta garanzia supplementare se il proprio profilo include software come servizio (SaaS), subappaltatori, hosting di siti Web o carte di pagamento.

Autocertificazione di DPR

Tutti i fornitori registrati nel programma SSPA devoto compilare un'autocertificazione di conformità DPR entro 90 giorni dopo averne ricevuta la richiesta. La richiesta sarà emessa annualmente ma potrà essere più frequente se il Profilo trattamento dati viene aggiornato a metà anno. Se si superano i 90 giorni, gli account dei fornitori passeranno allo stato SSPA Rosso (non in conformità). Nuovi ordini di acquisto non potranno essere processati finché lo stato SSPA non ritorni a Verde (in conformità).

I nuovi fornitori devono portare a termine i requisiti richiesti per garantire che il loro stato SSPA sia Verde (in conformità) primo di iniziare gli impegni.

Importante: il team SSPA non è autorizzato a rilasciare estensioni per questo compito.

I rappresentanti autorizzati che completano l'autocertificazione dovrebbero accertarsi di ricevere informazioni sufficienti dagli esperti in materia per rispondere con sicurezza a ogni requisito. Inoltre, apponendo il proprio nome al programma SSPA attestano di avere letto e compreso i DPR. I fornitori possono aggiungere altri contatti allo strumento online per aiutare il completamento dei requisiti.

Il Rappresentante autorizzato (vedere DPR per la definizione) deve:

1. Stabilire quali requisiti si applicano.
2. Postare una risposta per ogni requisito applicabile.
3. Firmare e inviare la certificazione nel Portale di conformità dei fornitori Microsoft.

Applicabilità

Ci si aspetta che i fornitori rispondano a tutti i requisiti DPR emessi a fronte del Profilo trattamento dati. È possibile che, tra quelli emessi, ci siano alcuni requisiti che non si applicano ai beni o servizi che il fornitore fornisce a Microsoft. Tali requisiti potranno essere contrassegnati come 'non applicabile' con commenti dettagliati che consentano la convalida da parte degli esaminatori SSPA.

I DPR inviati saranno esaminati dal team SSPA per convalidare ogni voce contrassegnata come 'non applicabile', 'conflitto legale locale' o 'conflitto contrattuale'. Il team SSPA potrà richiedere chiarimenti riguardo uno o più dei requisiti. I conflitti legali locali o di contratto saranno accettati solo se ci sono riferimenti di supporto e il conflitto è chiaro.

Requisito di valutazione indipendente

Per vedere quali approvazioni di trattamento dati attivano questo requisiti, vedere Requisiti secondo approvazione nell'Appendice A.

I fornitori possono scegliere di cambiare le approvazioni aggiornando il loro Profilo trattamento dati. Ma se ha un ruolo trattamento dati di "sub-responsabile trattamento dati", il fornitore non potrà modificare questa approvazione e dovrà sottoporsi annualmente a Valutazione indipendente.

Per garantire di ottenere le approvazioni che richiedono una verifica di conformità indipendente, i fornitori dovranno scegliere un valutatore indipendente che convalidi la conformità a fronte del DPR. Il valutatore dovrà compilare una lettera consultiva che garantisce la conformità a Microsoft. Tale lettera deve essere senza riserve e tutti i problemi di non conformità devono essere risolti e rimediati prima che la lettera di conferma sia inviata nel Portale di conformità dei fornitori Microsoft per esame da parte del team SSPA. I valutatori possono scaricare il modello di lettera consultiva allegato al PDF "Valutatori preferiti" disponibile qui.

Se si preferisce, quando applicabile, come in caso di fornitori di SaaS, fornitori di hosting di siti Web o fornitori con subappaltatori, non usare un valutatore indipendente per verificare la conformità nei confronti del DPR, si potrà utilizzare una delle certificazioni alternative accettabili trovate nella **Appendice A**. Le norme ISO 27701 (privacy) e ISO 27001 (sicurezza) sono affidabili per fornire requisiti vicini a quelli del DPR.

Qualora il fornitore sia o fornitore di assistenza sanitaria negli Stati Uniti, o entità coperta, la relazione HITRUST sarà accettata come prova di conformità a privacy e sicurezza.

Se le circostanze lo giustificano, SSPA potrà procedere a una valutazione indipendente manuale per effettuare dovuta diligenza. Ad esempio, in caso di richiesta per privacy e sicurezza della divisione, convalida di dati di rimedio incidente o requisito per l'esecuzione automatizzata dei diritti degli interessati.

Guida su come affrontare questo requisito:

1. L'incarico deve essere svolto da un valutatore con formazione tecnica e conoscenze in materia sufficienti per valutare adeguatamente la conformità.

2. I valutatori devono essere associati alla International Federation of Accountants (IFAC) o all'American Institute of Certified Public Accountants (AICPA), ovvero devono possedere la certificazione di un'altra pertinente organizzazione di privacy e sicurezza, come la International Association of Privacy Professionals (IAPP) o la Information Systems Audit and Control Association (ISACA).
3. Il valutatore deve usare il DPR più recente che include le prove richieste in supporto di ciascun requisito. **I fornitori dovranno fornire al valutatore le loro più recenti risposte di certificazione DPR approvato.**
4. Nel caso di fornitore di nuova iscrizione, l'ispettore comproverà la concezione dei controlli di processo. In tutti gli altri casi, il valutatore verificherà l'efficacia dei controlli.
5. L'ambito dell'incarico di valutazione è limitato ai dati personali e/o ai dati riservati di Microsoft in relazione alla Prestazione del fornitore.
6. L'ambito dell'incarico è limitato a tutte le attività di trattamento dati nell'ambito eseguite a fronte del numero di account fornitore che ha ricevuto la richiesta. Se il fornitore sceglie più di un account fornitore contemporaneamente, **la lettera di certificazione deve contenere l'elenco degli account fornitore inclusi nella valutazione e gli indirizzi corrispondenti.**
7. La lettera inviata a SSPA non deve contenere nessuna dichiarazione riguardante requisiti di protezione dei dati che il fornitore non soddisfa come specificati. Tali problemi dovranno essere corretti prima di poter inviare la lettera.

SSPA ha compilato una lista di valutatori preferiti disponibile. Queste aziende hanno familiarità con lo svolgimento di valutazioni SSPA. I fornitori sono tenuti a pagare per questa valutazione; i costi varieranno a seconda dell'estensione e della portata del trattamento dei dati.

Requisito di certificazione PCI DSS

Lo standard Payment Card Industry Data Security Standard (PCI DSS) rappresenta un framework per sviluppare una robusta sicurezza dei dati di carte di pagamento che include prevenzione, rilevamento e reazione adeguata agli incidenti di sicurezza. Il framework è stato sviluppato dal PCI Security Standards Council, un'organizzazione industriale di autoregolamentazione. Lo scopo dei requisiti PCI DSS consiste in identificare le vulnerabilità tecnologiche e di processo che mettono a rischio la sicurezza dei dati dei titolari di carta che vengono elaborati.

Microsoft deve conformarsi a questi standard. Quando un fornitore gestisce le informazioni della carta di pagamento per conto di Microsoft, Microsoft richiede la prova di adesione a questi standard. Vedere il PCI Security standards council per comprendere i requisiti imposti dall'organizzazione PCI.

A seconda del volume di transazioni trattate, il fornitore dovrà incaricare un Valutatore della sicurezza qualificato della certificazione o potrà compilare un modulo questionario di autovalutazione.

In genere, I marchi delle carte di pagamento stabiliscono le soglie per tipo di valutazione:

- Livello 1: fornire un certificato PCI AOC del valutatore di terza parte
- Livello 2 o 3: fornire un questionario di autovalutazione PCI DSS (SAQ) firmato dal funzionario del fornitore.

Inviare la certificazione applicabile che soddisfa i requisiti PCI.

Requisito Software come servizio

Ai fornitori che soddisfano la definizione SaaS inclusa nel Profilo trattamento dati potrebbe essere richiesto di fornire una certificazione ISO 27001 valida, se ciò è richiesto nel Contratto di servizi cloud di Microsoft.

I revisori SSPA verificheranno che la documentazione inviata soddisfi gli obblighi contrattuali.

Si prega di non inviare una certificazione del datacenter. Si prevede la certificazione ISO 27001 che si applica al(i) servizio(i) software indicato(i) nel contratto con Microsoft.

Uso di subappaltatori

Microsoft considera l'utilizzo di subappaltatori un fattore ad alto rischio. I fornitori che si servono di subappaltatori per trattare dati personali o dati riservati di Microsoft devono rendere noti tali subappaltatori. Inoltre, il fornitore dovrebbe rendere noti i Paesi in cui i dati personali saranno trattati da ogni subappaltatore.

Incidenti con i dati

Se viene a conoscenza di un incidente relativo alla privacy o ai dati di sicurezza, il fornitore deve informare Microsoft come dettagliato e definito nel DPR.

Segnalare gli incidenti con i dati servendosi di SupplierWeb o email a SuppIR@microsoft.com

Accertarsi di includere:

- Data dell'incidente con i dati:
- Nome del fornitore:
- Numero del fornitore:
- Contatto(i) di Microsoft notificato(i):
- Ordine di acquisto associato se applicabile/disponibile:
- Riepilogo dell'incidente con i dati:

Appendice A

Requisiti basati su approvazioni di profilo

#	Profilo	Requisiti di garanzia	Opzioni di garanzia indipendente
1	**Ambito:** personali, riservati **Sito trattamento dati:** presso Microsoft o il cliente **Ruolo di trattamento:** responsabile del trattamento o revisore **Classe dati:** riservati **o** altamente riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di subappaltatori:** non applicabile **Hosting di siti Web:** Non applicabile	Autocertificazione di conformità al DPR	
2	**Ambito:** riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** non applicabile **Classe dati:** riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di Subappaltatori:** non applicabile **Hosting di siti Web:** non applicabile	Autocertificazione di conformità al DPR	
3	**Ambito:** riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** Responsabile del trattamento **Classe dati:** altamente riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di subappaltatori:** non applicabile **Hosting di siti Web:** non applicabile	Autocertificazione di conformità al DPR **e** Garanzia di conformità indipendente	Opzioni di garanzia indipendente: 1. Completare una valutazione indipendente a fronte del DPR, **o** 2. Inviare ISO 27001

#	Profilo	Requisiti di garanzia	Opzioni di garanzia indipendente
4	**Ambito:** personali, riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** responsabile del trattamento **Classe dati:** altamente riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di subappaltatori:** non applicabile **Hosting di siti Web:** non applicabile	Autocertificazione di conformità al DPR **e** Garanzia di conformità indipendente	Opzioni di garanzia indipendente: 1. Completare una valutazione indipendente a fronte del DPR, 2. una valutazione indipendente a fronte delle sezioni A - I del DPR e di ISO 27001 **o** 3. inviare ISO 27701 **e** ISO 27001
5	**Ambito:** personali, riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** Responsabile del trattamento **Classe dati:** riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di Subappaltatori:** non applicabile **Hosting di siti Web:** non applicabile	Autocertificazione di conformità al DPR	
6	**Ambito:** personali, riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** Revisore **Classe dati:** altamente riservati o riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di Subappaltatori:** non applicabile **Hosting di siti Web:** non applicabile	Autocertificazione di conformità al DPR	

#	Profilo	Requisiti di garanzia	Opzioni di garanzia indipendente
7	**Ambito:** personali, riservati **Sito trattamento dati:** qualsiasi **Ruolo di trattamento:** Sub-responsabile del trattamento (questo ruolo viene determinato da Microsoft - il profilo dirà "Approvazione Sub-responsabile del trattamento: Sì") **Classe dati:** altamente riservati o riservati **Carte di pagamento:** non applicabile **SaaS:** non applicabile **Uso di Subappaltatori:** non applicabile **Hosting di siti Web:** non applicabile	Autocertificazione di conformità al DPR **e** Garanzia di conformità indipendente	Opzioni di garanzia indipendente: 1. Completare una valutazione indipendente a fronte del DPR, 2. una valutazione indipendente a fronte delle sezioni A - I del DPR e di ISO 27001 **o** 3. inviare ISO 27701 **e** ISO 27001

#	Profilo	Requisiti di garanzia	Opzioni di garanzia indipendente
Impatto dell'aggiunta di SaaS, subappaltatori, hosting di siti Web			
8	**Ambito:** personali, riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** Responsabile del trattamento **Classe dati:** altamente riservati o riservati **Carte di pagamento:** non applicabile **Subappaltatori:** SÌ o **SaaS:** SÌ o **Hosting di siti Web:** SÌ	Autocertificazione di conformità al DPR **e** Garanzia di conformità indipendente	Opzioni di garanzia indipendente: 1. Completare una valutazione indipendente a fronte del DPR, 2. una valutazione indipendente a fronte delle sezioni A - I del DPR e di ISO 27001 **o** 3. inviare ISO 27701 **e** ISO 27001
9	**Ambito:** personali, riservati **Sito trattamento dati:** presso il fornitore **Ruolo di trattamento:** Revisore **Classe dati:** altamente riservati o riservati **Carte di pagamento:** non applicabile **Subappaltatori:** SÌ o **SaaS:** SÌ o **Hosting di siti Web:** SÌ	Autocertificazione di conformità al DPR	

#	Profilo	Requisiti di garanzia	Opzioni di garanzia indipendente
Garanzia supplementare per carte di pagamento e SaaS			
10	Qualsiasi profilo sovrastante e **Carte di pagamento**	I requisiti sovrastanti applicabili **e** garanzia Payment Card Industry.	Inviare la certificazione PCI DSS
11	Qualsiasi profilo sovrastante e **Software come servizio (SaaS)**	I requisiti sovrastanti applicabili **e** invio di una certificazione ISO 27001 richiesta da contratto che copre i servizi funzionali.	Presentare una certificazione ISO 27001 con copertura funzionale del(i) servizio(i) fornito(i).