Requisiti di protezione dei dati per i fornitori Microsoft

Applicabilità

I requisiti per la protezione dei dati dei fornitori Microsoft ("**RPD**") si applicano a tutti i fornitori che elaborano dati personali di Microsoft o dati riservati di Microsoft in relazione alle loro prestazioni (ad es. fornitura di servizi, licenze software, servizi cloud) secondo i termini di questo contratto con Microsoft (ad es. termini dell'ordine di acquisto, contratto master) ("**Eseguire,**" "**Esecuzione**" o "**Prestazioni**").

- In caso di conflitto tra i requisiti qui contenuti e i requisiti specificati negli accordi tra il fornitore e Microsoft, l'RPD ha la precedenza a meno che il fornitore applicabile non identifichi nel modulo di attestazione dell'RPD la fornitura corretta che entra in conflitto con la sezione dell'RPD applicabile (in tale caso, i termini del contratto prevalgono).
- In caso di conflitto tra i requisiti qui contenuti e qualsiasi requisito legale o normativo, questi ultimi avranno la precedenza.
- Se il fornitore Microsoft opera come titolare del trattamento, relativamente a questo RPD, valgono solo i requisiti nella sezione Sicurezza J e Gestione A riguardo alle attività di trattamento del fornitore.
- Se il fornitore di Microsoft non elabora i dati personali, ma solo i dati riservati, di Microsoft, relativamente a questo RPD, si applicano solo i requisiti nella sezione Gestione A, Conservazione E e Sicurezza J riguardo al trattamento dei dati riservati di Microsoft.

Trasferimento internazionale di dati

Senza limitazione agli altri obblighi, il fornitore non effettuerà alcun trasferimento internazionale dei dati personali di Microsoft laddove Microsoft non abbia fornito previo consenso scritto, e dovrà in ogni caso adempiere ai requisiti in materia di protezione dei dati di qualsiasi termine contrattuale standard, regolamento aziendale vincolante o altra disposizione approvata da qualsivoglia autorità di protezione dei dati, il Comitato europeo per la protezione dei dati o la Commissione europea e adottati o concordati da Microsoft, ivi compresa la norma EU-U.S e la norma Swiss-U.S. Privacy Shield e il regolamento generale europeo sulla protezione dei dati. Il fornitore accetta di contattare Microsoft nel caso in cui decida di non poter più rispettare l'impegno preso nell'offrire lo stesso livello di protezione stabilito dai principi della Privacy Shield. Il fornitore dovrà inoltre assicurarsi che qualsivoglia subresponsabile adempierà agli stessi requisiti (come definito nella clausola 1(d) del documento Clausole contrattuali standard pubblicato nel 2010 come allegato alla Decisione della Commissione europea C(2010)593).

Definizioni chiave

I seguenti termini usati in questo RPD avranno i seguenti significati. Gli esempi che seguono i termini "inclusi", "quali", "ad esempio", o simili utilizzati all'interno di questo RPD vanno interpretati includendo "senza limitazione" o "ma non in via esclusiva", salvo diversamente specificato da termini quali "solo" o "esclusivamente".

Per "**dati personali di Microsoft**" si intendono tutte le informazioni personali elaborate da o per conto di Microsoft.

Per "**dati personali**" si intendono tutte le informazioni riguardanti una persona fisica identificata o identificabile ("**soggetto interessato**"); una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificatore, ad esempio nome, numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più elementi specifici relativi all'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di quella persona fisica.

Per “**dati riservati di Microsoft**” si intendono tutte le informazioni che, se divulgate o danneggiate, possono comportare significativi danni economici o di immagine per Microsoft. Sono inclusi prodotti hardware e software di Microsoft, applicazioni line-of-business interne, materiali di marketing precedenti il rilascio di prodotti, codici di licenza e documentazione tecnica correlata ai prodotti e servizi Microsoft.

Per “**diritto del soggetto interessato**” si intende il diritto di un soggetto di accedere ai propri dati personali Microsoft, eliminarli, modificarli, esportarli, limitarne il trattamento o opporsi a esso se richiesto dalla legge.

Per “**legge**” si intendono tutte le leggi, i regolamenti, gli statuti, i decreti, le decisioni, gli ordini, le decisioni, i codici, gli atti legislativi, le risoluzioni e i requisiti di qualsiasi autorità governativa (federale, statale, loca,e o internazionale) avente giurisdizione. Per “**illecito**” si intende qualsiasi violazione della legge.

Per “**responsabile del trattamento**” si intende la persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altra entità che tratta i dati personali per conto del titolare del trattamento.

Per “**titolare del trattamento**” si intende la persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altra entità che da sola o insieme ad altri determina gli scopi e i mezzi del trattamento dei dati personali; laddove gli scopi e i mezzi del trattamento sono determinati dall'Unione europea (“**UE**”) o dalla legislazione degli Stati membri, il titolare del trattamento (o i criteri per la nomina del titolare del trattamento) può essere designato da tale legislazione.

Per “**trattamento**” si intende qualsiasi operazione o insieme di operazioni compiute sui dati personali o riservati di Microsoft con o senza l’ausilio di processi automatizzati, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione. “Trattamento” e “trattato” hanno lo stesso significato.

Per “**violazione dei dati**” si intende la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione A: Gestione		
1	Qualsiasi accordo applicabile fra Microsoft e il fornitore (ad es. contratto master, commessa o ordine di acquisto e altri ordini) contiene termini specifici della protezione della privacy e della sicurezza dei dati rispetto ai dati riservati e personali di Microsoft, secondo quanto applicabile. Per le aziende che operano come responsabili del trattamento, l'accordo deve includere l'oggetto e la durata del trattamento, la natura e lo scopo del trattamento, il tipo di dati personali di Microsoft e le categorie di soggetti interessati, e gli obblighi e i diritti di Microsoft.	Il fornitore deve presentare il contratto applicabile fra Microsoft e il fornitore. Per i Responsabili del trattamento, le descrizioni del Trattamento sono contenute nell'accordo applicabile (*ad es.* commessa o ordine di acquisto). Nota: le aziende che hanno ordini di acquisto in corso troveranno la descrizione delle attività di trattamento aggiunta successivamente nel corso del processo di acquisto.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
2	Assegnare la responsabilità del rispetto dell'RPD a una persona o a un team specifico della propria azienda.	Il nome della persona o del gruppo incaricato di garantire la conformità all'RPD del fornitore Microsoft. Un documento che descrive l'autorità e le responsabilità di questa persona o gruppo attestante un ruolo legato alla privacy e/o alla sicurezza.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
3	Stabilire, mantenere ed eseguire la formazione annuale sulla privacy e la sicurezza per i dipendenti che avranno accesso ai dati personali e riservati di Microsoft. Se l'azienda non ha preparato alcun documento, usare questo profilo della storyboard e adattarlo alla propria azienda.	Sono disponibili record annuali di partecipazione. I contenuti della formazione includono principi di privacy e sicurezza.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
4	Trattare i dati personali di Microsoft soltanto su istruzione documentata di Microsoft, anche in caso di trasferimento di dati personali di Microsoft verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda la legge; in tal caso, il responsabile del trattamento (fornitore) informa il titolare del trattamento (Microsoft) circa tale obbligo giuridico prima del trattamento stesso, a	Prova documentata delle istruzioni come stabilito da un contratto (ad esempio una commessa o un ordine di acquisto), o acquisito come parte di un sistema elettronico usato nella fornitura dei servizi.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

	meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.		

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione B: Avviso		
5	Nel raccogliere i dati personali per conto di Microsoft, il fornitore deve fare riferimento all'informativa sulla privacy di Microsoft. Le comunicazioni sulla privacy devono essere chiare e disponibili al fine di consentire agli interessati di decidere se inviare i propri dati personali al fornitore. Nota: quando l'azienda è il titolare del trattamento, pubblicherà la propria informativa sulla privacy. *Contattare SSPAHelp@microsoft.com per accedere alle corrette informative Microsoft.*	Il fornitore utilizza un collegamento all'informativa sulla privacy Microsoft attuale pubblicata. L'informativa sulla privacy è pubblicata in qualsiasi contesto in cui saranno raccolti i dati personali degli utenti. Se presente, viene messa a disposizione una versione offline fornita prima della raccolta dei dati. Le informative sulla privacy offline utilizzate sono le ultime versioni pubblicate, debitamente datate. Per i servizi ai dipendenti Microsoft, viene utilizzata la comunicazione sulla protezione dei dati di Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
6	I fornitori che raccolgono dati personali di Microsoft nel corso di telefonate registrate o conversazioni dal vivo devono essere preparati a esporre ai soggetti interessati le prassi di raccolta, gestione, uso e conservazione dei dati applicabili.	Uno script per le registrazioni vocali include le modalità di elaborazione dei dati personali di Microsoft e di ▪ raccolta, ▪ utilizzo e ▪ conservazione.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione C: Scelta e consenso		
7	Qualora il fornitore si serva del consenso come base giuridica per il trattamento dei dati, deve ottenere e registrare il consenso della persona interessata per tutte le proprie attività di trattamento (inclusa qualsiasi attività di trattamento nuova e aggiornata) prima di raccoglierne i dati personali.	Il fornitore può dimostrare in che modo un soggetto fornisce l'autorizzazione a un'attività di trattamento e che l'autorizzazione riguarda tutte le attività di trattamento del fornitore rispetto ai dati personali di quel soggetto. Il fornitore può dimostrare in che modo un soggetto può ritirare la propria autorizzazione all'attività di trattamento. Il fornitore può dimostrare in che modo vengono espresse le preferenze prima dell'avvio di una nuova attività di trattamento. Il fornitore monitora l'efficacia della gestione delle preferenze per garantire che vengano rispettate le tempistiche necessarie per recepire la modifica di una preferenza secondo la normativa locale più rigida vigente. Nota: esempi di prove sono gli screenshot delle interazioni con l'utente, la sperimentazione del servizio o l'opportunità di visualizzare la documentazione tecnica.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione C: Scelta e consenso (segue)		
8	I cookie sono piccoli file di testo memorizzati sui dispositivi da siti Web e/o applicazioni online che contengono le informazioni usate per riconoscere un soggetto o un dispositivo. I fornitori che creano e gestiscono siti Web e applicazioni Microsoft devono inviare ai soggetti un avviso di trasparenza e consentir loro di poter scegliere se usare i cookie. I fornitori che creano e gestiscono siti Web e/o applicazioni Microsoft devono garantire che l'uso dei cookie sia in linea con quanto dichiarato nell'informativa sulla privacy di Microsoft e con i requisiti legali come le norme stabilite dall'UE.	Lo scopo di ogni cookie deve essere documentato e l'utente deve essere informato sul tipo di cookie implementato. ▪ Quando i cookie di sessione sono sufficienti, non devono essere usati cookie persistenti. ▪ Quando vengono usati cookie persistenti, la loro data di scadenza non deve superare i 2 anni da quando l'utente ha visitato il sito. Per gli utenti dell'UE, la data di scadenza per un cookie persistente non deve superare i 13 mesi. Confermare la conformità alle leggi UE come richiesto, ad esempio tramite ▪ l'uso delle convenzioni di etichettatura, "Privacy e cookie" per l'informativa sulla privacy, e ▪ garantire il consenso dell'utente prima dell'uso di cookie per scopi "non essenziali" come la pubblicità.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione D: Raccolta		
9	Il fornitore deve monitorare la raccolta di dati personali e/o riservati di Microsoft al fine di garantire che siano raccolti solo i dati necessari a erogare il servizio richiesto da Microsoft.	Il fornitore può presentare una documentazione che attesta che i dati personali e/o riservati di Microsoft raccolti sono necessari ai fini del servizio.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
10	Qualora si procuri dati personali da terze parti per conto di Microsoft, il fornitore deve verificare che le politiche e le prassi sulla protezione dei dati applicate dalla terza parte siano compatibili con il proprio contratto con Microsoft e con l'RPD.	Il fornitore può dimostrare di operare in modo diligente relativamente alle politiche e alle prassi di protezione dei dati di terze parti.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
11	Prima di raccogliere dati personali di Microsoft mediante l'installazione o l'impiego di un software eseguibile sul dispositivo del soggetto interessato, la necessità di disporre di tali informazioni dovrà essere documentata in un contratto per fornitore in vigore con Microsoft.	Il consenso di Microsoft a usare software eseguibile sul dispositivo del soggetto interessato è riportato nel contratto in vigore.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
12	Prima di raccogliere dati personali di Microsoft sensibili (dati che rivelano l'origine razziale o etnica, le opinioni politiche, le credenze religiose o le idee filosofiche, o l'appartenenza a sindacati, dati genetici, dati biometrici, dati relativi alla salute o dati riguardanti la vita sessuale o l'orientamento sessuale di una persona fisica) è necessario documentare la necessità di raccogliere questi dati in un contratto per il fornitore in vigore con Microsoft.	La necessità di raccogliere i dati personali di Microsoft sensibili è riportata nel contratto in vigore con Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione E: Conservazione		
13	Garantire che i dati personali e riservati di Microsoft siano conservati solo per il tempo strettamente necessario a fornire i servizi, a meno che il loro mantenimento continuativo sia richiesto dalla legge.	Il fornitore rispetta le politiche di conservazione documentate o i requisiti di conservazione specificati da Microsoft nel contratto (ad es. nella commessa o nell'ordine di acquisto).	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
14	Garantire che, al termine delle prestazioni o su richiesta di Microsoft, i dati personali e riservati di Microsoft in possesso o sotto il controllo del fornitore siano distrutti o restituiti a Microsoft (a esclusiva discrezione di questa). All'interno delle applicazioni, devono essere in atto procedure per garantire che al momento della rimozione dei dati dall'applicazione, eseguita in modo esplicito dagli utenti o sulla base di altri fattori quali il periodo di conservazione dei dati, questi vengano eliminati in modo sicuro. Qualora dovesse risultare necessario distrugge i dati personali e riservati di Microsoft, il fornitore deve bruciare, polverizzare o sminuzzare i supporti fisici contenenti i dati personali e/o confidenziali Microsoft in modo tale che questi non possano essere più letti o ricostruiti.	Conservare i dati sulla cessione dei dati personali e riservati di Microsoft (per esempio restituzione a Microsoft per distruzione). Se la distruzione è necessaria o richiesta da Microsoft, fornire un certificato di distruzione firmato da un rappresentante del fornitore.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione F: Soggetti interessati		
	I soggetti interessati hanno diritto di accedere, eliminare, modificare, esportare, limitare e opporsi al trattamento dei dati personali ("**Diritti dei soggetti interessati**"). Quando un soggetto interessato si propone di esercitare i propri diritti secondo la legge applicabile relativa ai dati personali di Microsoft, il fornitore deve:		
15	Collaborare con Microsoft, tramite misure tecniche e organizzative adeguate, per quanto possibile, affinché possa rispettare il proprio obbligo di rispondere alle richieste dei soggetti interessati che desiderano esercitare i loro diritti.	Sono in atto processi e le procedure per supportare l'esecuzione dei diritti dei soggetti interessati.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
16	Rispondere a tutte le richieste relative ai diritti del soggetto interessato in modo puntuale.	Il fornitore deve effettuare dei test periodici per assicurarsi di poter sostenere i diritti dei soggetti interessati.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
17	A meno che Microsoft non abbia dato istruzioni diverse, il fornitore farà riferimento a tutti i soggetti interessati che contattano il fornitore direttamente al fine di consentire a Microsoft di far rispettare i diritti del soggetto interessato. Il fornitore comunicherà al soggetto interessato le operazioni da effettuare per ottenere accesso o altrimenti esercitare i propri diritti rispetto ai dati personali di Microsoft. *Contattare SSPAHelp@microsoft.com per ricevere assistenza su questo requisito.*	Il fornitore deve comunicare la procedura da seguire per accedere ai dati personali, nonché a tutti metodi disponibili per aggiornare i dati.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
18	Quando si risponde direttamente al soggetto interessato, è necessario verificare l'identità del soggetto interessato che effettua la richiesta.	Il fornitore ha documentato il metodo usato per identificare i soggetti interessati Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione F: Soggetti interessati (segue)		
	Una volta autenticata l'identità del soggetto interessato il fornitore deve:		
19	Determinare se detiene o controlla i dati personali di Microsoft relativi a tale soggetto interessato.	Il fornitore ha implementato procedure per stabilire se i dati personali sono stati trattenuti.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
20	Adoperarsi in ogni ragionevole modo per reperire i dati personali di Microsoft richiesti e mantenere record sufficienti a dimostrare di aver effettuato una ricerca opportuna.	Il fornitore conserva un record per dimostrare la procedura seguita per soddisfare le richieste relative ai diritti del soggetto interessato. La documentazione include, ▪ data e ora della richiesta, ▪ azioni intraprese per rispondere alla richiesta e ▪ record di quanto Microsoft è stata informata.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
21	Registrare la data e l'ora delle richieste relative ai diritti del soggetto interessato, nonché le misure intraprese in risposta a tale richiesta. Fornire a Microsoft, su richiesta di questa, i record del soggetto interessato.	Il fornitore deve conservare i record delle richieste di accesso e documentare le modifiche apportate ai dati personali.	
	Dopo aver accertato l'identità del soggetto interessato e aver controllato di disporre dei dati personali Microsoft richiesti, il fornitore deve:		
22	Per le richieste di una copia dei dati personali, fornire i dati personali di Microsoft al soggetto interessato in un formato appropriato cartaceo, elettronico o tramite comunicazione verbale.	Il fornitore deve fornire al soggetto interessato i dati personali in un formato comprensibile e in una forma comoda per il soggetto interessato e per il fornitore.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
23	In caso di diniego della richiesta da parte della direzione di Microsoft, fornire al soggetto interessato una spiegazione scritta conforme a tutte le eventuali istruzioni in merito precedentemente distribuite da Microsoft.	Documentare le istanze in cui le richieste vengono rifiutate e conservare le prove di revisione ed approvazione di Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

	Contattare SSPAHelp@microsoft.com per ricevere assistenza su questo requisito.		
#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione F: Soggetti interessati (segue)		
24	Il fornitore deve adottare ogni ragionevole precauzione per garantire che i dati personali di Microsoft rilasciati a un soggetto interessato non possano essere utilizzati per identificare un'altra persona.	Il fornitore deve dimostrare che sono state prese le opportune precauzioni per impedire l'identificazione di un'altra persona a partire dalle informazioni rilasciate (per esempio deve garantire che non sia possibile fotocopiare l'intera pagina dei dati se i dati personali richiesti per un soggetto interessato compaiono solo su una riga).	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
25	In caso di disaccordo tra il fornitore e il soggetto interessato circa la completezza e l'accuratezza dei dati personali di Microsoft, il fornitore deve demandare la questione a Microsoft e cooperare con questa nella misura necessaria per risolverla. *Contattare SSPAHelp@microsoft.com per ricevere assistenza su questo requisito.*	Il fornitore deve documentare le istanze di disaccordo e inoltrare il problema a Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione G: Divulgazione a terzi		
	Qualora intenda servirsi di un subappaltatore che lo coadiuvi nel trattamento dei dati personali e riservati di Microsoft, il fornitore deve:		
26	Ottenere l'espresso consenso scritto di Microsoft prima di subappaltare i servizi o apportare modifiche riguardanti l'aggiunta o la sostituzione dei subappaltatori. *Contattare SSPAHelp@microsoft.com per ricevere assistenza su questo requisito.*	Confermare che i dati personali di Microsoft sono trattati solo da aziende note a Microsoft, come previsto da contratto applicabile (ad es. commessa, addendum, ordine d'acquisto) o conservato nel database di SSPA.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
27	Documentare la natura e l'entità dei dati personali e riservati di Microsoft trattati dai subappaltatori, assicurando che le informazioni raccolte sono necessarie per l'erogazione dei servizi.	Il fornitore deve mantenere la documentazione relativa ali dati personali e riservati di Microsoft divulgati o trasferiti ai subappaltatori.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
28	Accertarsi che il subappaltatore usi i dati personali di Microsoft conformemente al metodo di contatto preferito indicato dal soggetto interessato.	Dimostrare in che modo una preferenza del soggetto interessato viene usata dai subappaltatori. Fornire documentazione di supporto che include il periodo di tempo entro il quale il subappaltatore deve recepire la modifica di una preferenza.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
29	Limitare il trattamento dei dati personali di Microsoft da parte del subappaltatore agli scopi necessari ad adempiere al contratto del fornitore con Microsoft.	Il fornitore può presentare una documentazione che attesta che i dati personali di Microsoft forniti a un subappaltatore sono necessari ai fini del servizio.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
30	Esaminare i reclami in merito al trattamento non autorizzato o illegale dei dati personali di Microsoft.	Il fornitore può dimostrare che sono in atto sistemi e procedure per indirizzare i reclami relativi all'uso o alla divulgazione non autorizzati dei dati personali Microsoft da parte di un subappaltatore.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione G: Divulgazione a terzi (segue)		
31	Informare tempestivamente Microsoft qualora si venga a sapere che un subappaltatore ha trattato i dati personali e riservati di Microsoft per qualsiasi scopo differente da quelli relativi all'erogazione dei servizi.	Il fornitore ha messo a disposizione le istruzioni e i mezzi necessari affinché il subappaltatore possa riportare usi impropri dei dati di Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
32	Intervenire prontamente per mitigare i danni potenziali o effettivi derivanti dal trattamento non autorizzato o illegale dei dati personali e riservati di Microsoft da parte del subappaltatore.	Il fornitore può dimostrare di poter attuare un piano e procedure in caso di uso improprio dei dati personali e riservati di Microsoft da parte di un subappaltatore.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
	Sezione H: Qualità		
33	Il fornitore deve mantenere l'integrità di tutti i dati personali di Microsoft, garantendo che siano accurati, completi e rilevanti al fine dichiarato per il quale sono stati trattati.	Il fornitore può dimostrare che sono in atto procedure per confermare i dati personali di Microsoft quando vengono raccolti, creati e aggiornati. Il fornitore può dimostrare che sono in atto procedure di monitoraggio e campionatura per verificare su basi costanti l'accuratezza e attuare correzioni secondo necessità.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione I: Monitoraggio e applicazione delle norme		
34	Il fornitore ha un piano di risposta all'incidente che gli richiede di informare Microsoft in modo puntuale non appena venga a conoscenza di una violazione dai dati o vulnerabilità della sicurezza in relazione alla gestione dei dati personali o riservati di Microsoft da parte del fornitore. *Contattare SSPAHelp@microsoft.com per riportare un incidente.*	Il fornitore ha un piano di risposta all'incidente che include una fase di notifica ai clienti (Microsoft) come descritto in questa sezione.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
35	Non rilasciare comunicati stampa o altri annunci pubblici riguardanti violazioni che coinvolgono i dati personali o riservati di Microsoft senza previa autorizzazione di Microsoft, salvo se imposto dalla legge.	Il fornitore acconsente a soddisfare questo requisito qualora si verifichi tale circostanza.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
36	Implementare un piano correttivo e monitorare le soluzioni adottate contro le violazioni o le vulnerabilità dei dati personali e/o riservati di Microsoft per assicurarsi che vengano intraprese azioni correttive appropriate con tempistiche adeguate.	Il fornitore ha a disposizione procedure documentate da adottare per rispondere a una violazione dei dati.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
37	Stabilire una procedura formale per rispondere a tutti i reclami in merito a protezione dei dati di cui siano oggetto i dati personali di Microsoft.	Il fornitore ha i mezzi per ricevere reclami riguardanti i dati personali di Microsoft e ha a disposizione una procedura documentata per rispondere ai reclami.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza		
	Il fornitore deve stabilire, implementare e mantenere un programma di sicurezza dei dati che includa le politiche e le procedure, al fine di proteggere e mantenere sicuri i dati personali e riservati di Microsoft, conformemente alle pratiche consigliate di settore e in base a quanto previsto dalla legge. Il programma di sicurezza del fornitore deve soddisfare gli standard elencati di seguito, ovvero i requisiti da 38 a 56.	Le protezioni possono essere superiori a quelle elencate, per necessità di osservanza degli schemi normativi (ad esempio HIPPA, GLBA) o dei requisiti contrattuali. Un rapporto ISO 27001 o SOC 2 valido è un sostituto accettabile della Sezione J. Contattare SSPAHelp@microsoft.com per applicare tale sostituzione. Nota: occorre fornire la documentazione che descrive la portata di tali certificazioni/rapporti.	
38	Eseguire valutazioni annuali sulla sicurezza di rete che includono: ▪ la revisione delle principali modifiche all'ambiente, ad esempio un nuovo componente di sistema, una topologia di rete, una regola firewall; ▪ le analisi delle vulnerabilità; e ▪ la conservazione dei registri delle modifiche.	Il fornitore ha documentato valutazioni di rete, registri delle modifiche e risultati delle analisi. I log delle modifiche richiesti devono riportare le modifiche, fornire informazioni sul motivo delle modifiche e includere nome e titolo della persona incaricata dell'approvazione.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
39	Il fornitore deve definire, comunicare e implementare una politica per i dispositivi mobili che protegga e limiti l'uso dei dati personali e riservati di Microsoft a cui si ha accesso o che sono usati su un dispositivo mobile.	Il fornitore dimostra l'uso di una politica sui dispositivi mobili conformi qualora l'elaborazione dei dati personali e riservati di Microsoft richiedano l'uso di un dispositivo mobile.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
40	Tutte le risorse usate per supportare l'erogazione dei servizi devono essere giustificate e avere un proprietario identificato. Il fornitore è responsabile del mantenimento di un inventario di tali risorse di informazioni, della definizione di un uso accettabile e autorizzato delle risorse e del mantenimento di un adeguato livello di protezione per le risorse durante tutto il ciclo di vita.	Inventario delle risorse relative ai dispositivi usate per supportare le prestazioni. L'inventario di tali risorse deve includere: ▪ la posizione del dispositivo; ▪ la classificazione dei dati nelle risorse; ▪ un record per il recupero delle risorse in caso di risoluzione del contratto di impiego o del contratto commerciale; e ▪ un record per lo smaltimento dei supporti di archiviazione dei dati quando non più necessari.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
41	Stabilire e mantenere le procedure di gestione dei diritti di accesso per evitare l'accesso non autorizzato ai dati personali e riservati di Microsoft controllati dai fornitori.	Il fornitore dimostra di aver implementato un piano di gestione dei diritti di accesso che include: ▪ procedure di controllo d'accesso; ▪ procedure di identificazione; ▪ procedure di blocco in seguito a tentativi falliti; ▪ reimpostazione della password con la frequenza necessaria ma non superiore ai 90 giorni; ▪ parametri affidabili per la selezione delle credenziali di autenticazione; e ▪ disattivazione degli account utente entro 48 ore dalla terminazione del rapporto di lavoro. Il fornitore dimostra di aver stabilito un processo per controllare l'accesso dell'utente ai dati personali e riservati di Microsoft, applicando il principio dei privilegi minimi. Il processo include: ▪ ruoli utente ben definiti; ▪ procedure per esaminare e giustificare l'approvazione di accesso ai ruoli; e ▪ la prova che gli utenti all'interno dei ruoli con accesso ai dati di Microsoft dispongano di una giustificazione documentata per la loro presenza nel gruppo/ruolo.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
42	La definizione e l'introduzione di procedure di gestione delle patch che privilegiano le patch di sicurezza per i sistemi usati nel trattamento dei dati personali e riservati di Microsoft includono: Tali procedure includono: ▪ un approccio ai rischi definito per dare priorità alle patch di sicurezza; ▪ la capacità di gestire e implementare le patch di emergenza; ▪ l'applicabilità al sistema operativo e al software del server ad esempio il server applicazioni e il software del database; ▪ la documentazione relativa al rischio mitigato dalle patch e le tracce di eventuali eccezioni; e ▪ i requisiti per il ritiro del software non più supportato dall'azienda produttrice.	Il fornitore può dimostrare di avere implementato una procedura di gestione delle patch che soddisfa questo requisito e copre almeno i seguenti aspetti. ▪ Assegnazione della gravità per indicare le priorità. (Le definizioni di gravità sono documentate.) ▪ Procedura documentata per implementare le patch di emergenza. ▪ Confermare che non siano in uso sistemi operativi non più supportati dall'azienda produttrice. ▪ Record di gestione delle patch che tengono traccia delle approvazioni e delle eccezioni.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
43	Installare software anti-virus e anti-malware sugli apparecchi collegati alla rete usata per trattare i dati personali e riservati di Microsoft, che comprendono i server, i desktop di produzione e formazione che proteggono da virus potenzialmente dannosi ed applicazioni software nocivi. Aggiornare le definizioni anti-malware ogni giorno o in base alle indicazioni del fornitore del software anti-virus/anti-malware. Nota: si applica a tutti i sistemi operativi incluso Linux.	Sono disponibili record che attestano che l'uso di software anti-virus e anti-malware è attivo. Nota: questo requisito si applica a tutti i sistemi operativi.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
44	I fornitori che sviluppano software per Microsoft devono includere principi di security-by-design nel processo di generazione.	I documenti delle specifiche tecniche del fornitore includono nei loro cicli di sviluppo punti di controllo della convalida di sicurezza.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
45	Adottare un programma di prevenzione della perdita dei dati ("**DLP**"). I dati devono essere classificati, etichettati e protetti adeguatamente e il fornitore deve monitorare i sistemi di informazioni in uso dove vengono trattati i dati personali e riservati di Microsoft per evitare le intrusioni, le perdite e altre attività non autorizzate. Il programma DLP, come minimo, ▪ richiede l'uso di sistemi di rilevamento delle intrusioni ("**IDS**") in host standard di settore, in rete e cloud-based se si conservano dati personali o riservati di Microsoft, ▪ richiede l'implementazione di sistemi di protezione delle intrusioni ("**IPS**") avanzati configurati per monitorare e interrompere attivamente la perdita di dati, ▪ nel caso in cui un sistema venga violato, è necessario effettuare l'analisi del sistema per assicurarsi di risolvere eventuali vulnerabilità residue, ▪ descrivere le procedure per il monitoraggio degli strumenti di rilevamento di un sistema compromesso e ▪ stabilire un processo di gestione e risposta all'incidente da eseguire quando viene rilevato un evento di violazione dei dati.	IDS/IPS documentati implementati con le procedure adottate per fornire una risposta in caso di rilevamento di una vulnerabilità o violazione dei dati.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
46	Comunicare tempestivamente i risultati delle indagini della risposta all'incidente ai reparti di gestione senior e a Microsoft. *Contattare SSPAHelp@microsoft.com per informare Microsoft.*	Devono essere in atto sistemi e procedure per comunicare i risultati dell'investigazione della risposta all'incidente a Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
47	Gli amministratori di sistema, il personale operativo, il management e le terzi parti devono seguire ogni anno un corso di formazione sulla sicurezza.	Stabilire un programma di formazione sulla sicurezza che includa: ▪ formazione annuale per la risposta agli incidenti; e ▪ eventi simulati e meccanismi automatici per facilitare una risposta efficace alle situazioni di crisi. Informazioni sulla prevenzione degli incidenti quali i rischi associati derivanti dal download di un software dannoso.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
48	Il fornitore deve garantire che le procedure di backup proteggano i dati personali e riservati di Microsoft dall'uso, dall'accesso, dalla divulgazione, dall'alterazione e dalla distruzione non autorizzati.	Il fornitore può documentare le procedure di risposta e ripristino indicando le modalità in cui l'organizzazione gestirà un evento imprevisto e manterrà la sicurezza delle informazioni a un livello prestabilito in base agli obiettivi di continuità per la sicurezza delle informazioni approvati dal reparto di gestione. Il fornitore può dimostrare di aver definito e implementato le procedure per eseguire periodicamente un backup, conservare in modo sicuro e recuperare in modo efficace i dati critici.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
49	Stabilire e verificare i piani di continuità aziendale e ripristino di emergenza.	Un piano di ripristino di emergenza deve includere quanto segue: ▪ criteri definiti per determinare se un sistema è critico per il funzionamento del business del fornitore; ▪ elenchi di sistemi critici sulla base dei criteri definiti a cui si deve fare riferimento per il ripristino in caso di emergenza; ▪ procedure di ripristino di emergenza definite per ciascun sistema critico che garantiscono il ripristino di un applicazione persino per un ingegnere che non conosce il sistema in meno di 72 ore. ▪ Eseguire test e controlli annuali (o più frequenti) dei piani di ripristino di emergenza per garantire il raggiungimento degli obiettivi di ripristino.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
50	Autenticare l'identità di un individuo prima di concedergli accesso ai dati personali o ai dati riservati di Microsoft.	Garantire che tutti gli ID utente siano univoci e che ognuno di essi abbia un metodo di autenticazione in base agli standard di settore quale Azure Active Directory. Per l'accesso con privilegi elevati (privilegi amministrativi o altri tipi di privilegi avanzati) è necessario l'uso di un secondo fattore, ad esempio una smart card o un autenticatore basato sul telefono.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
51	Il fornitore deve proteggere i dati personali o riservati di Microsoft in transito sulle reti con crittografia che usano Transport Layer Security ("**TLS**") o Internet Protocol Security ("**IPsec**"). Questi metodi sono descritti in NIST 800-52 e NIST 800-57; può essere usato anche uno standard di settore equivalente. Il fornitore deve rifiutarsi di comunicare qualsiasi dato personale o riservato di Microsoft trasmesso tramite mezzi non codificati.	È necessario definire e applicare il processo di creazione, distribuzione e sostituzione del TLS o di altri certificati.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
52	Tutti dispositivi del fornitore (computer portatili, workstation, ecc.) che potranno accedere a dati personali o informazioni riservate di Microsoft e gestirli devono usare la crittografia basata su disco.	Crittografare tutti i dispositivi per soddisfare i requisiti di Bitlocker o di un'altra soluzione di settore equivalente per la crittografia del disco per tutti i dispositivi client usati per gestire i dati personali e riservati di Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
53	È necessario attuare sistemi e procedure per crittografare i dati personali di Microsoft, indicati di seguito, inattivi (quando sono archiviati) usando standard di settore attuali quali quello descritto nello standard NIST 800-111: ▪ dati delle credenziali (ad es. nome utente/password) ▪ dati usati come strumento di pagamento (ad esempio numeri di carte di credito e conti bancari) ▪ dati personali relativi all'immigrazione ▪ dati sul profilo medico (ad es. numeri delle cartelle mediche o marcatori o identificatori biometrici, come DNA, impronte digitali, retine e iridi, pattern vocali e facciali e misure delle mani, usati a scopo identificativo) ▪ dati di identificazione emessi da autorità governative (ad es. numero di sicurezza sociale o della patente di guida) ▪ dati appartenenti ai clienti Microsoft (ad es. Sharepoint, documenti O365, clienti One drive) ▪ materiale relativo a prodotti Microsoft non annunciati ▪ Data di nascita ▪ Informazioni sui profili dei bambini ▪ dati geografici in tempo reale ▪ indirizzo fisico personale (non aziendale) ▪ numeri di telefono personali (non aziendali) ▪ religione ▪ opinioni politiche ▪ orientamento/preferenze sessuali ▪ risposte alle domande di sicurezza (ad es. 2fa, reimpostazione password) o nome da nubile della madre	Verificare che i dati personali e riservati di Microsoft elencati in questa riga siano crittografati inattivi.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
54	Quando si trattano i dati di carte di credito per conto di Microsoft, rispettare le norme applicabili per la gestione delle carte di credito per ciascuna azienda o emittente della carta.	Dimostrare la conformità producendo annualmente una certificazione Payment Card Industry Data Services Standard ("**PCI-DSS**"). *Presentare le certificazioni PCI DSS a SSPA. Contattare SSPAHelp@microsoft.com* per qualsiasi domanda.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*

#	Requisiti di protezione dei dati per i fornitori Microsoft	Prova di conformità	Risposta
	Sezione J: Sicurezza (segue)		
55	Il fornitore deve conservare le risorse fisiche Microsoft in un ambiente con accesso controllato.	Devono essere in atto sistemi e procedure per gestire l'accesso fisico a copie digitali, fisiche, di archivio e di backup dei dati personali di Microsoft. È necessario tracciare la catena di custodia relativa al movimento e alla distruzione dei supporti fisici contenenti i dati di Microsoft.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*
56	Rendere anonimi tutti i dati personali di Microsoft utilizzati in ambiente di test o di sviluppo.	I dati personali di Microsoft non devono essere usati negli ambienti di sviluppo o test. Qualora non vi sia alternativa, devono essere resi anonimi per evitare l'identificazione dei soggetti interessati o l'uso improprio dei dati personali. Nota: i dati resi anonimi sono diversi dai dati con pseudonimo. I dati resi anonimi sono dati che non fanno riferimento a una persona fisica identificata o identificabile laddove il soggetto dei dati personali non è o non è più identificabile.	*<Conforme>* *<Non conforme>* *<Non applicabile>* *<Conflitto legale>* *<Conflitto contrattuale>*