Requisiti di protezione dei dati dei fornitori Microsoft

Rilevanza

I requisiti di protezione dei dati dei fornitori Microsoft (nel prosieguo i "**DPR**") hanno rilevanza per ciascun fornitore Microsoft che tratti i dati personali di Microsoft o i dati riservati di Microsoft in relazione alle prestazioni di tale fornitore (ad esempio, fornitura di servizi, licenze software, servizi cloud) in base ai termini del suo accordo con Microsoft (ad esempio, condizioni dell'ordine di acquisto, accordo quadro) (nel prosieguo "**Eseguire**", "**Esecuzione**" o "**Prestazione**").

- In caso di conflitto tra i DPR e i requisiti specificati negli accordi contrattuali tra il fornitore e Microsoft, i DPR prevalgono a meno che il fornitore non identifichi la disposizione corretta all'interno dell'accordo che sostituisce il requisito di protezione dei dati applicabile (in tal caso, a prevalere sono i termini dell'accordo).
- In caso di conflitto tra i requisiti contenuti nel presente documento ed eventuali requisiti legali o statutari, prevalgono i requisiti legali o statutari.
- Nel caso in cui il fornitore Microsoft operi come titolare del trattamento, al fornitore potrebbero essere applicati dei requisiti ridotti, rispetto ai DPR.
- Nel caso in cui il fornitore Microsoft non tratti i dati personali di Microsoft ma solo i dati riservati di Microsoft, al fornitore potrebbero essere applicati dei requisiti ridotti, rispetto a questi DPR.

Trasferimento internazionale dei dati

Senza limitazione di altri suoi obblighi, il fornitore non effettuerà alcun trasferimento internazionale di dati personali di Microsoft a meno che non venga fornita una preventiva approvazione scritta da parte di Microsoft e, in ogni caso, il fornitore dovrà rispettare i requisiti di protezione dei dati, comprese le clausole contrattuali standard, o, a discrezione di Microsoft, altri meccanismi di trasferimento transfrontaliero adeguati e approvati da un'autorità per la protezione dei dati preposta o dalla Commissione europea, a seconda dei casi, e adottati o accettati da Microsoft. Clausole contrattuali standard sostitutive adottate da (i) Commissione europea o dal Garante europeo della protezione dei dati e approvate dalla Commissione europea, (ii) Regno Unito ai sensi della Legge federale generale sulla protezione dei dati del Regno Unito, (iii) Svizzera ai sensi della Legge federale svizzera sulla protezione dei dati, o (iv) tali clausole che disciplinano il trasferimento internazionale di dati personali ufficialmente adottate da un governo in una giurisdizione diversa dalla Svizzera, dal Regno Unito e dalle giurisdizioni che costituiscono l'Unione Europea/Spazio economico europeo, che devono essere integrate e vincolanti per il fornitore a partire dal giorno della loro adozione. Il fornitore dovrà inoltre garantire che tutti i sub-responsabili (come definiti nelle clausole contrattuali standard) si conformino a loro volta.

Definizioni chiave

I seguenti termini utilizzati nei presenti DPR hanno i seguenti significati. Un elenco di esempi che segua i termini "compreso", "come", "ad esempio", "per esempio" o altri termini simili utilizzati in tutto il presente documento, sono interpretati in modo da includere "senza limitazione" o "ma non limitato a" a meno che non siano qualificati da parole come "solo" o "esclusivamente". Per le altre definizioni, consultare il glossario alla fine del presente documento.

"**Titolare del trattamento**" indica l'entità che determina le finalità e i mezzi del trattamento dei dati personali. "Titolare del trattamento" include un'azienda, un titolare del trattamento (come definito nel GDPR) e i termini equivalenti utilizzati nelle leggi sulla protezione dei dati, come richiesto dal contesto.

I "**cookie**" sono piccoli file di testo memorizzati sui dispositivi dai siti web e/o dalle applicazioni, e contengono informazioni utilizzate per riconoscere un interessato dal trattamento o un dispositivo.

"**Violazione dei dati**" indica (1) una violazione della sicurezza che provoca la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali di Microsoft o ai dati riservati di Microsoft trasmessi, archiviati

o altrimenti trattati dal fornitore o dai suoi subappaltatori, o (2) la vulnerabilità della sicurezza relativa alla gestione da parte del fornitore dei dati personali di Microsoft o dei dati riservati di Microsoft.

"**Interessato**" indica una persona fisica identificabile che può essere identificata, direttamente o indirettamente, in particolare facendo riferimento a un identificatore, come un nome, un numero di documento d'identità, dati relativi all'ubicazione, un identificativo online o a uno o più fattori specifici d'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica.

"**Diritti dell'interessato**" indica il diritto di un interessato di accedere, eliminare, modificare, esportare, limitare o di opporsi al trattamento dei dati personali Microsoft di tale interessato, se richiesto dalla legge.

"**Legge**" indica tutte le leggi, le norme, gli statuti, i decreti, le decisioni, gli ordini, i regolamenti, le sentenze, i codici, gli atti, le risoluzioni e i requisiti applicabili emanati da qualsiasi autorità governativa (federale, statale, locale o internazionale) avente giurisdizione. "**Illegale**" indica qualsiasi violazione della legge.

I "**dati riservati di Microsoft**" sono tutte le informazioni la cui compromissione, in termini di riservatezza o integrità, può comportare una significativa perdita reputazionale o finanziaria per Microsoft. Ciò include i prodotti hardware e software di Microsoft, le applicazioni settoriali interne, i materiali di marketing non pubblicati, le chiavi di licenza del prodotto e la documentazione tecnica relativa ai prodotti e ai servizi Microsoft.

"**Dati personali di Microsoft**" indica qualsiasi dato personale trattato da o per conto di Microsoft.

"**Dati personali**" indica qualsiasi informazione relativa a un interessato e qualsiasi altra informazione che costituisca "dati personali" o "informazioni personali" ai sensi di legge.

"**Trattare**" indica qualsiasi operazione o insieme di operazioni eseguite su dati personali o riservati di Microsoft, con o senza l'ausilio di processi automatizzati, come raccogliere, registrare, organizzare, strutturare, conservare, adattare o modificare, estrarre, consultare, utilizzare, divulgare mediante trasmissione e diffusione o altrimenti rendere disponibile, uniformare o interconnettere, limitare, cancellare o distruggere. "Trattamento" e "Trattato" hanno significati corrispondenti.

"**Responsabile del trattamento**" indica un'entità che tratta i dati personali per conto di un'altra entità e include il fornitore di servizi, il responsabile del trattamento (come definito nel GDPR) e i termini equivalenti utilizzati nelle leggi sulla protezione dei dati, come richiesto dal contesto.

"**Subappaltatore**" indica un soggetto terzo a cui il fornitore delega i propri obblighi in relazione all'accordo a copertura della propria Prestazione, inclusa un'affiliata del fornitore non contrattualmente legata a Microsoft in modo diretto.

"**Sub-responsabile**" indica un soggetto terzo che Microsoft assume per eseguire, laddove la Prestazione includa il trattamento dei dati personali di Microsoft per il quale Microsoft è un responsabile del trattamento.

Risposta del fornitore

Annualmente, i fornitori confermeranno la propria conformità a questi requisiti utilizzando un servizio online amministrato da Microsoft. Per capire come viene gestita la conformità, consultare la Guida al programma SSPA.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione A - Gestione	
1	Ciascun accordo applicabile tra Microsoft e il fornitore (ad esempio, l'accordo quadro, il capitolato, gli ordini di acquisto e altri ordini) contiene indicazioni sulla protezione dei dati in materia di privacy e sicurezza, in relazione ai dati personali e riservati di Microsoft, a seconda dei casi, inclusi i divieti di vendita dei dati personali di Microsoft e del loro trattamento al di fuori del rapporto commerciale diretto tra Microsoft e il fornitore. Per le società che operano in qualità di responsabili o sub-responsabili del trattamento in relazione alla Prestazione, in relazione ai dati personali Microsoft, l'accordo deve includere l'oggetto e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali di Microsoft e le categorie degli interessati e gli obblighi e i diritti di Microsoft.	Il fornitore è tenuto a presentare l'accordo applicabile tra Microsoft e il fornitore. Per i responsabili e i sub-responsabili del trattamento, la descrizione del trattamento è contenuta nell'accordo applicabile (ad esempio, il capitolato, gli ordini di acquisto). Nota: le società con ordini di acquisto in corso potranno ricevere la necessaria descrizione del trattamento in una fase successiva del processo di acquisto.
2	Laddove Microsoft confermi che gli impegni della società danno luogo a un ruolo di sub-responsabile, il fornitore deve avere appropriati accordi in essere con Microsoft sulla protezione dei dati. Nota: in un tale caso, Microsoft pubblicherà questa designazione sul profilo della società.	Clausole contrattuali standard, appendice sui dati dei clienti online e/o appendice sul trattamento dei dati per i servizi professionali di fornitori e partner.
3	Assegnazione delle responsabilità per la conformità ai DPR a una persona o un gruppo designato all'interno della società.	Indicazione del ruolo della persona o del gruppo incaricato di garantire la conformità ai DPR dei fornitori di Microsoft. Un documento che descriva l'autorità e la responsabilità di questa persona o gruppo, che comprovi un ruolo legato a privacy e/o sicurezza.
4	Istituzione, mantenimento e svolgimento di una formazione annuale sulla privacy e sulla sicurezza per i dipendenti che avranno accesso ai dati personali trattati dal fornitore in relazione alle prestazioni o ai dati riservati di Microsoft. Se la società non dispone di contenuti già predisposti, potrà utilizzare questo modello di scenario e adattarlo all'utilizzo appropriato per la società. Nota: al personale del fornitore potrebbe venir chiesto di seguire ulteriori corsi di formazione, forniti dalle divisioni Microsoft.	I dati annuali sulle presenze sono disponibili e possono essere forniti a Microsoft su richiesta. I contenuti della formazione includono i principi di privacy e sicurezza. La documentazione relativa alla conformità ai requisiti di formazione includerà le prove di una formazione sui requisiti normativi della privacy, sugli obblighi di sicurezza e sul rispetto dei requisiti e degli obblighi contrattuali applicabili.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione A - Gestione (continua)	
5	Trattamento dei dati personali di Microsoft solo in conformità con le istruzioni documentate di Microsoft, inclusi gli scenari relativi ai trasferimenti dei dati personali di Microsoft verso un Paese terzo o un'entità internazionale, a meno che ciò non sia richiesto dalla legge. In tal caso, il responsabile o il sub-responsabile (fornitore) informerà il titolare del trattamento (Microsoft) dell'esistenza di tale requisito legale prima di procedere al trattamento, a meno che la legge in questione non vieti una tale notifica per importanti motivi di interesse pubblico.	Il fornitore compila e conserva in forma elettronica tutte le istruzioni documentate ricevute da Microsoft (ad esempio, l'accordo, il capitolato o documentazione relativa all'ordine) in un luogo facilmente accessibile ai dipendenti e appaltatori del fornitore che partecipano alla Prestazione.
	Sezione B - Notifica	
6	Il fornitore deve attenersi all'informativa sulla privacy di Microsoft quando raccoglie i dati personali per conto di Microsoft. Tale informativa sulla privacy deve essere facilmente disponibile per gli interessati al fine di aiutarli a decidere se inviare i propri dati personali al fornitore. Nota: laddove la società sia il titolare delle attività di trattamento, dovrà pubblicare la sua informativa sulla privacy.	Il fornitore utilizza un link di inoltro all'attuale informativa sulla privacy pubblicata da Microsoft. L'informativa sulla privacy viene pubblicata in qualsiasi contesto in cui verranno raccolti i dati personali di un utente. Ove applicabile, è disponibile una versione offline che viene fornita prima della raccolta dei dati. L'eventuale informativa sulla privacy offline utilizzata è l'ultima versione pubblicata e opportunamente datata. Per i servizi per i dipendenti Microsoft, viene utilizzata l'informativa sulla privacy dei dati di Microsoft.
7	Quando si raccolgono i dati personali di Microsoft tramite una chiamata vocale dal vivo o registrata, i fornitori devono essere preparati a illustrare agli interessati le pratiche di raccolta, gestione, utilizzo e conservazione di tali dati.	Un copione per le registrazioni vocali include il modo in cui vengono trattati i dati personali di Microsoft e comprende: ▪ la raccolta, ▪ l'utilizzo e ▪ la conservazione

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione C - Scelta e consenso	
8	Ove applicabile, prima di raccogliere i dati personali dell'interessato, il fornitore dovrà ottenere e registrare il consenso dell'interessato per tutte le attività di trattamento (incluse eventuali attività di trattamento nuove e aggiornate). Il fornitore monitora l'efficacia della gestione delle preferenze espresse dagli interessati per garantire che il periodo di tempo necessario per onorare una modifica delle preferenze corrisponda al requisito legale locale più restrittivo.	Il fornitore è in grado di dimostrare in che modo un interessato fornisce il suo consenso per un'attività di trattamento e che l'ambito del consenso copre tutte le attività di trattamento del fornitore in relazione ai dati personali dell'interessato. Il fornitore è in grado di dimostrare il modo in cui un interessato revoca il suo consenso per un'attività di trattamento. Il fornitore è in grado di dimostrare come vengono verificate le preferenze prima dell'avvio di una nuova attività di trattamento. Nota: le possibili prove possono essere le schermate di interazione dell'utente, l'esperienza con il servizio o la possibilità di visionare la documentazione tecnica.
9	I fornitori che creano e gestiscono siti web e/o applicazioni di Microsoft o siti che portano il marchio Microsoft, devono mettere a disposizione degli interessati un avviso e una scelta trasparenti in merito all'utilizzo dei cookie, in linea con gli impegni nell'informativa sulla privacy di Microsoft e con i requisiti legali locali. Per gestire la verifica delle scelte, se non espressamente vietato dall'unità aziendale appaltante, i fornitori dovranno utilizzare il banner standard prodotto da 1ES. Questo requisito si applica nel caso in cui i siti si rivolgano a utenti all'interno dell'Unione Europea/Spazio economico europeo e in altre aree geografiche dove vigono leggi sulla privacy e ovunque venga utilizzata l'informativa sulla privacy di Microsoft. Nota: gli sponsor aziendali di Microsoft devono registrare i siti Microsoft nel portale interno per la conformità web (http://aka.ms/wcp) per catalogare e gestire l'inventario dei cookie.	Lo scopo di ciascun cookie deve essere documentato e devono essere fornite informazioni sul tipo di cookie implementato. ▪ I cookie persistenti non devono essere utilizzati quando sono sufficienti quelli di sessione. ▪ I cookie persistenti utilizzati non devono avere una data di scadenza superiore a 13 mesi dopo che l'utente ha visitato il sito. Deve essere garantita la conformità alle leggi vigenti dell'UE, come ad esempio: ▪ utilizzo della convenzione di etichettatura, "Privacy e Cookie" per l'informativa sulla privacy, ▪ garanzia di consenso affermativo dell'utente prima dell'utilizzo di cookie "non essenziali" per scopi quali pubblicità, e ▪ durata del consenso non superiore a 6 mesi e obbligo di rinnovo del consenso a tale scadenza.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione D - Raccolta	
10	Il fornitore deve monitorare la raccolta dei dati personali e/o riservati di Microsoft per garantire che gli unici dati raccolti siano quelli necessari per Eseguire.	Il fornitore è in grado di fornire la documentazione che dimostri che i dati personali e/o riservati di Microsoft raccolti sono necessari per Eseguire. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
11	Prima di raccogliere dei dati da minori (come stabilito dalla giurisdizione pertinente), il fornitore deve ottenere il consenso in base alle leggi locali sulla privacy.	Il fornitore è in grado di fornire la documentazione che mostri il consenso di un genitore/tutore. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
	Sezione E - Conservazione	
12	Garanzia che i dati personali e riservati di Microsoft vengano conservati per un periodo non superiore a quello necessario per l'Esecuzione, a meno che la legge non richieda che vengano conservati a tempo indeterminato.	Il fornitore si attiene alle politiche di conservazione documentate o ai requisiti di conservazione specificati da Microsoft nell'accordo (ad esempio, il capitolato, l'ordine di acquisto). Il fornitore produrrà le prove documentali su richiesta di Microsoft.
13	Garanzia che, a esclusiva discrezione di Microsoft, i dati personali e riservati di Microsoft in possesso del fornitore, o sotto il suo controllo, vengano restituiti a Microsoft o distrutti al compimento della Prestazione o su richiesta di Microsoft. All'interno delle applicazioni è necessario che siano previsti dei processi che garantiscono l'eliminazione sicura dei dati che vengono rimossi dall'applicazione in modo esplicito dagli utenti o in base ad altri automatismi, come la loro data di scadenza. Quando si rende necessaria la distruzione dei dati personali o riservati di Microsoft, il fornitore deve bruciare, polverizzare o distruggere i supporti fisici che contengono i dati personali e/o riservati di Microsoft in modo che le informazioni non possano essere né lette né ricostruite.	Tenere un registro di eliminazione dei dati personali e riservati di Microsoft (ciò può includere la restituzione a Microsoft per la distruzione). Se la distruzione viene richiesta da Microsoft, fornire un certificato di distruzione firmato da un funzionario del fornitore.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione F - Interessati	
	Gli interessati godono di determinati diritti ai sensi della legge, che includono il diritto di accedere, eliminare, modificare, esportare, limitare e opporsi al trattamento dei propri dati personali (nel prosieguo i "**Diritti dell'interessato**"). Quando un interessato richiede di esercitare i propri diritti ai sensi della legge, in relazione ai propri dati personali di Microsoft, il fornitore deve mettere Microsoft in condizione di eseguire quanto necessario o eseguire direttamente tali attività per conto di Microsoft.	
14	Ove possibile, assistere Microsoft, mediante adeguate misure tecniche e organizzative, nell'adempimento dei suoi obblighi di risposta alle richieste degli interessati che richiedono di esercitare i propri diritti di interessato senza indebito ritardo. Per l'esercizio dei loro diritti dell'interessato, il fornitore indirizzerà tutti gli interessati che lo contattano direttamente a Microsoft, a meno di indicazione diversa da parte di Microsoft.	Il fornitore conserverà le prove dei processi e delle procedure documentati a supporto dell'esecuzione dei diritti dell'interessato. Il fornitore conserverà anche le prove documentate dei test. Tali prove saranno rese disponibili su richiesta di Microsoft.
15	Qualora risponda direttamente all'interessato o fornisca un meccanismo self-service online, il fornitore dovrà disporre processi e procedure finalizzati a identificare l'interessato che effettua la richiesta.	Il fornitore avrà documentato tale metodo utilizzato per identificare gli interessati di Microsoft. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
16	Se Microsoft chiede di individuare i dati personali di Microsoft relativi a un interessato che non sono disponibili tramite un meccanismo self-service online, il fornitore farà ogni ragionevole sforzo per individuare i dati richiesti e conserverà registrazioni sufficienti per dimostrare che è stata effettuata una ricerca ragionevole.	Il fornitore conserverà le prove documentate delle procedure in atto per stabilire se i dati personali di Microsoft sono conservati e fornirà la relativa documentazione su richiesta di Microsoft. Il fornitore terrà un registro delle misure adottate per soddisfare le richieste relative ai diritti dell'interessato. Tale documentazione include: ▪ la data e l'ora della richiesta, ▪ le azioni intraprese per rispondere alla richiesta e l'annotazione di quando Microsoft è stata informata. Il fornitore produrrà le prove documentali su richiesta di Microsoft.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione F - Interessati (continua)	
17	Il fornitore comunicherà all'interessato i passi da seguire per ottenere l'accesso o per esercitare i propri diritti in relazione ai propri dati personali di Microsoft.	Il fornitore conserverà le prove documentate delle comunicazioni e delle procedure per l'accesso ai dati personali di Microsoft. Il fornitore conserverà le prove documentate e le fornirà a Microsoft su richiesta.
18	Registrazione della data e dell'ora delle richieste relative ai diritti dell'interessato e le azioni intraprese dal fornitore in risposta a tali richieste. Se la richiesta dell'interessato viene respinta, su indicazione di Microsoft, fornire all'Interessato una spiegazione scritta. Fornire le registrazioni relative alle richieste dell'interessato a Microsoft su richiesta.	Il fornitore conserverà le registrazioni relative alle richieste di accesso/cancellazione e documenterà le modifiche apportate ai dati personali di Microsoft. Documentare le istanze in cui le richieste vengono rifiutate e conservare le prove della revisione e dell'approvazione di Microsoft. Il fornitore fornirà la prova della tenuta dei registri di richieste e rifiuti in relazione all'accesso ai dati personali di Microsoft.
19	Il fornitore deve permettere a Microsoft o ottenere una copia dei dati personali di Microsoft richiesti per l'interessato autenticato in un formato cartaceo, elettronico o verbale appropriato.	Il fornitore metterà a disposizione i dati personali di Microsoft all'interessato in un formato comprensibile e comodo sia per l'interessato che per il fornitore.
20	Il fornitore dovrà adottare ragionevoli precauzioni per garantire che i dati personali di Microsoft rilasciati a Microsoft o a un interessato autenticato non possano essere utilizzati per identificare una terza persona.	Il fornitore conserverà le prove documentate delle procedure relative a tali precauzioni finalizzate a evitare l'identificazione dell'interessato contrariamente ai termini dell'Accordo. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
21	Se un interessato ritiene che i propri dati personali di Microsoft non siano completi e accurati, il fornitore dovrà inoltrare la questione a Microsoft e collaborare con Microsoft, se necessario, per risolvere il problema.	Il fornitore documenterà le istanze di disaccordo e inoltrerà la questione a Microsoft. Il fornitore produrrà le prove documentali su richiesta di Microsoft.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione G - Subappaltatori	
	Se il fornitore intende affidarsi a un subappaltatore per trattare i dati personali o riservati di Microsoft, il fornitore dovrà:	
22	Notificare anticipatamente Microsoft dell'intenzione di subappaltare i servizi o apportare modifiche relative all'aggiunta o alla sostituzione di subappaltatori. Nota: esprimere l'accettazione di questo obbligo anche se attualmente non ci si affida ad alcun subappaltatore, in quanto ciò potrebbe accadere in futuro.	Confermare che i dati personali di Microsoft vengano trattati esclusivamente da società note a Microsoft come richiesto nell'accordo applicabile (ad esempio, il capitolato, l'appendice, l'ordine di acquisto) o acquisiti nel database SSPA. Il fornitore può pubblicare il proprio elenco di subappaltatori online e includere un link alla pagina nel database SSPA.
23	Documentare la natura e l'entità dei dati personali e riservati di Microsoft trattati dai subappaltatori, garantendo che le informazioni raccolte siano necessarie per l'Esecuzione.	Il fornitore conserverà la documentazione relativa ai dati personali e riservati di Microsoft divulgati o trasferiti ai subappaltatori. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
24	Laddove Microsoft sia un titolare del trattamento dei dati personali di Microsoft, garantire che il subappaltatore utilizzi i dati personali di Microsoft in conformità con le preferenze di contatto dichiarate dall'interessato.	Dimostrare come le preferenze dell'interessato di Microsoft siano utilizzate dai subappaltatori. Fornire una documentazione di supporto (ad esempio, istantanee dello schermo, SLA, SOW, ecc.) che includa il periodo di tempo necessario per onorare una modifica delle preferenze da parte del subappaltatore.
25	Limitare il trattamento dei dati personali o riservati di Microsoft da parte del subappaltatore a quanto necessario per adempiere all'accordo del fornitore con Microsoft.	Il fornitore deve essere in grado di fornire la documentazione che dimostri che i dati personali di Microsoft forniti al subappaltatore sono necessari per l'Esecuzione. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
26	Esaminare i reclami per individuare qualsiasi trattamento non autorizzato o illegale dei dati personali di Microsoft.	Il fornitore è in grado di dimostrare l'attuazione di sistemi e processi finalizzati a rispondere ai reclami relativi all'uso o alla divulgazione non autorizzati dei dati personali di Microsoft da parte di un subappaltatore. Il fornitore produrrà le prove documentali su richiesta di Microsoft.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione G - Subappaltatori (continua)	
27	Avviso tempestivo a Microsoft non appena si apprende che un subappaltatore ha trattato i dati personali o riservati di Microsoft per scopi diversi da quelli relativi alla Prestazione.	Il fornitore avrà fornito istruzioni e mezzi a un subappaltatore per segnalare l'uso improprio dei dati Microsoft. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
28	Se il fornitore raccoglie dati personali tramite soggetti terzi per conto di Microsoft, dovrà confermare che le politiche e le pratiche di protezione dei dati di tali soggetti terzi sono coerenti con l'accordo del fornitore con Microsoft e con i DPR.	Il fornitore è in grado di fornire la documentazione relativa alla due diligence svolta in merito alle politiche e alle pratiche di protezione dei dati di soggetti terzi. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
29	Intraprendere tempestivamente le azioni necessarie per mitigare qualsiasi danno effettivo o potenziale causato da un trattamento non autorizzato o illegale da parte di un subappaltatore di dati personali e riservati di Microsoft.	Il fornitore deve conservare le prove documentali del piano e della procedura attuati e fornire prove della documentazione a Microsoft su richiesta.
	Sezione H - Qualità	
30	Il fornitore dovrà mantenere l'integrità di tutti i dati personali di Microsoft, garantendo che siano sempre accurati, completi e pertinenti per gli scopi dichiarati per i quali sono stati trattati.	Il fornitore è in grado di dimostrare che esistono procedure atte a ratificare i dati personali di Microsoft quando vengono raccolti, creati e aggiornati. Il fornitore è in grado di dimostrare che esistono procedure di monitoraggio e campionamento atte a verificare l'accuratezza su base continuativa e a effettuare correzioni, ove necessario. Il fornitore produrrà le prove documentali su richiesta di Microsoft.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione I - Monitoraggio e applicazione	
31	Il fornitore dispone di un piano di risposta in caso di violazione che prevede la notifica a Microsoft in base ai requisiti contrattuali o, senza indebito ritardo, non appena viene a conoscenza di una violazione dei dati, a seconda di quale dei due casi si verifica per primo. Il fornitore deve, su richiesta o indicazione di Microsoft, collaborare con Microsoft in qualsiasi indagine, mitigazione o rimedio della violazione dei dati, compreso il dotare Microsoft dei dati, delle informazioni, dell'accesso al personale del fornitore o del hardware necessario per condurre una revisione forense. Nota: per la procedura di notifica a Microsoft in caso di violazione, vedere la Guida al programma SSPA.	Il fornitore dispone di un piano di risposta in caso di violazione che prevede un percorso di notifica ai clienti (Microsoft), come descritto in questa sezione. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
32	Attuazione di un piano di rimedio e monitorare la risoluzione di ciascuna violazione dei dati per garantire che vengano adottate tempestivamente le azioni correttive appropriate.	Il fornitore dispone di procedure documentate utili a rispondere a una violazione dei dati, fino alla loro risoluzione. Il fornitore produrrà le prove documentali su richiesta di Microsoft.
33	Laddove Microsoft sia un titolare del trattamento dei dati personali di Microsoft, istituire una procedura di reclamo formale che risponda a tutti i reclami sulla protezione dei dati che coinvolgono i dati personali di Microsoft.	Il fornitore dispone dei mezzi per ricevere i reclami che coinvolgono i dati personali di Microsoft e dispone di una procedura di reclamo documentata per affrontare tali reclami. Il fornitore produrrà le prove documentali su richiesta di Microsoft.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione J - Sicurezza	
	Il fornitore deve istituire, attuare e gestire un programma di sicurezza delle informazioni che includa politiche e procedure atte a proteggere e mantenere protetti i dati personali e riservati di Microsoft, in conformità con le buone pratiche del settore e come richiesto dalla legge. Il programma di sicurezza messo in atto dal fornitore deve soddisfare gli standard riportati di seguito: requisiti da 34 a 50.	Una certificazione ISO 27001 valida è un sostituto accettabile per la sezione J. Contattare SSPA per procedere a questa sostituzione. Nota: si dovrà fornire la certificazione.
34	Esecuzione di valutazioni annuali della sicurezza della rete che includono: ▪ revisione dei principali cambiamenti nell'ambiente di rete, come un nuovo componente di sistema, topologia della rete, regole del firewall, ▪ esecuzione di scansioni di vulnerabilità e ▪ tenuta di registri delle modifiche.	Il fornitore avrà documentato le valutazioni della rete, i registri delle modifiche e i risultati delle scansioni. I registri delle modifiche richiesti dovranno tenere traccia delle modifiche, contenere informazioni sul motivo della modifica e includere il nome e il titolo dell'approvatore designato.
35	Il fornitore deve stabilire, comunicare e attuare una politica sui dispositivi mobili che protegga e limiti l'uso dei dati personali o riservati di Microsoft a cui si accede o che vengono utilizzati su un dispositivo mobile.	Laddove il trattamento dei dati personali o riservati di Microsoft richieda l'uso di un dispositivo mobile, il fornitore dimostrerà l'attuazione di una politica per dispositivi mobili conforme.
36	Tutte le risorse utilizzate a supporto della Prestazione devono essere contabilizzate ed essere associate un proprietario identificato. Il fornitore è responsabile della tenuta di un inventario di tali risorse informative; di stabilire un loro uso accettabile e autorizzato; e di fornire un livello appropriato di protezione per le risorse durante tutto il loro ciclo di vita.	Inventario dei dispositivi utilizzati a supporto della Prestazione. L'inventario di tali dispositivi includerà: ▪ ubicazione del dispositivo, ▪ classificazione dei dati presenti sull'unità, ▪ registrazione del recupero dell'unità alla cessazione del rapporto di lavoro o del contratto commerciale, e ▪ registrazione dello smaltimento dei supporti di archiviazione dei dati non più necessari.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione J - Sicurezza (continua)	
37	Istituzione e attuazione di procedure di gestione dei diritti di accesso al fine di impedire accessi non autorizzati a qualsiasi dato personale o riservato di Microsoft che si trovi sotto il controllo del fornitore.	Il fornitore dimostrerà di aver attuato un piano di gestione dei diritti di accesso che include: ▪ procedure di verifica degli accessi, ▪ procedure di identificazione, ▪ procedure di blocco a seguito di tentativi di accesso falliti, ▪ rigidi parametri per la selezione delle credenziali di autenticazione, ▪ disattivazione degli account dell'utente entro 48 ore, in caso di cessazione del rapporto di lavoro, e ▪ severi controlli delle password che impongano la sua lunghezza e complessità e ne impediscano il riutilizzo. Il fornitore dimostrerà di disporre di una procedura consolidata per l'esame degli accessi degli utenti ai dati personali e riservati di Microsoft, applicando il principio del privilegio minimo. Tale procedura prevede: ▪ ruoli degli utenti chiaramente definiti, ▪ procedure di revisione e giustificazione dell'approvazione di accesso ai ruoli, e ▪ verifica che gli utenti all'interno dei ruoli con accesso ai dati di Microsoft dispongano di una giustificazione documentata per far parte di tale gruppo o ruolo.
38	Definizione e attuazione di procedure di gestione delle patch che diano priorità alle patch di sicurezza per i sistemi utilizzati per il trattamento dei dati personali o riservati di Microsoft. Tali procedure prevedono: ▪ un approccio al rischio stabilito in modo da dare priorità alle patch di sicurezza, ▪ la capacità di gestire e implementare patch di emergenza, ▪ l'applicabilità al sistema operativo e al software del server, come ad esempio il server applicativo e il software del database, ▪ la documentazione del rischio mitigato dalla patch e tracciamento di eventuali eccezioni, e ▪ i necessari requisiti per il ritiro del software non più supportato dalla relativa società di sviluppo.	Il fornitore è in grado di dimostrare l'attuazione di una procedura di gestione delle patch che soddisfi questo requisito e copra, come minimo, quanto segue: ▪ assegnazione del livello di gravità per attivare la definizione delle priorità (le definizioni del livello di gravità sono documentate), ▪ procedura documentata di implementazione delle patch di emergenza, ▪ conferma che non vengono utilizzati sistemi operativi non più supportati dalla società di sviluppo, e ▪ registrazioni della gestione delle patch che tracciano le approvazioni e le eccezioni.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione J - Sicurezza (continua)	
39	Installazione di software antivirus e antimalware sulle apparecchiature connesse alla rete utilizzate per trattare i dati personali e riservati di Microsoft, inclusi server, desktop di produzione e formazione per la protezione da virus e altri software potenzialmente maligni e dannosi. Aggiornamento quotidiano delle definizioni antimalware o come indicato dal fornitore dell'antivirus o dell'antimalware. Nota: ciò vale per tutti i sistemi operativi, incluso Linux.	Esistenza di registrazioni che dimostrano che i software antivirus e antimalware sono attivi. Nota: questo requisito vale per tutti i sistemi operativi.
40	I fornitori che sviluppano software per Microsoft devono incorporare i principi di sicurezza in base alla progettazione nel processo di sviluppo.	I documenti delle specifiche tecniche dei fornitori includeranno punti di controllo che confermino la sicurezza durante i loro cicli di sviluppo.
41	Impiego di un programma di prevenzione della perdita di dati (nel prosieguo "**DLP**") che prevenga le intrusioni, la perdita di dati e altre attività non autorizzate. I dati devono essere adeguatamente classificati, etichettati e protetti e il fornitore deve monitorare i sistemi informatici con i quali vengono trattati i dati personali o riservati di Microsoft per prevenire intrusioni, perdite e altre attività non autorizzate. Il programma DLP deve come minimo: ▪ richiedere l'uso di sistemi di rilevamento delle intrusioni basati su host, rete e cloud, standard del settore (nel prosieguo "**IDS**"), se vengono conservati i dati personali o riservati di Microsoft, ▪ richiedere l'implementazione di sistemi avanzati di protezione dalle intrusioni (nel prosieguo "**IPS**") configurati per monitorare e impedire attivamente la perdita di dati, ▪ richiedere, in caso di violazione di un sistema, l'analisi del sistema per garantire che vengano affrontate anche eventuali vulnerabilità residue, ▪ descrivere le procedure necessarie per monitorare gli strumenti di rilevamento della compromissione del sistema, ▪ il fornitore determina una risposta alle violazioni e un processo di gestione da eseguire quando viene rilevata una violazione dei dati, e	Programma DLP documentato installato con procedure in atto per prevenire le intrusioni, la perdita di dati e altre attività non autorizzate (e almeno tutti gli elementi specificati in questa sezione).

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione J - Sicurezza (continua)	
	▪ richiedere comunicazioni (a tutti i dipendenti del fornitore e ai subappaltatori esclusi dalla Prestazione del fornitore) in merito al download e all'utilizzo non autorizzato dei dati personali o riservati di Microsoft.	
42	Comunicare tempestivamente i risultati dell'indagine derivanti dalla risposta alle violazioni ai responsabili senior e a Microsoft.	Devono essere attuati sistemi e processi per comunicare i risultati dell'indagine derivanti dalla risposta alle violazioni a Microsoft.
43	Gli amministratori di sistema, il personale operativo, i responsabili e i soggetti terzi devono seguire una formazione annuale sulla sicurezza.	Istituzione di un programma di formazione sulla sicurezza che includa: ▪ formazione annuale sulla risposta alle violazioni, ▪ eventi simulati e meccanismi automatizzati per facilitare una risposta efficace agli scenari di crisi, e ▪ consapevolezza della prevenzione delle violazioni, come i rischi collegati al download di software dannoso.
44	Il fornitore deve garantire che i processi di pianificazione del backup proteggano i dati personali e riservati di Microsoft da uso, accesso, divulgazione, alterazione e distruzione non autorizzati.	Il fornitore è in grado di dimostrare l'esistenza di procedure documentate di risposta e ripristino che descrivono in dettaglio come l'azienda gestirà un evento perturbatore e come manterrà la sicurezza delle informazioni a un livello predeterminato, in base agli obiettivi di continuità della sicurezza delle informazioni approvati dalla direzione. Il fornitore è in grado di dimostrare di aver stabilito e attuato delle procedure per eseguire periodicamente il backup, l'archiviazione sicura e il recupero efficace dei dati critici.
45	Istituzione e verifica dei piani per la continuità aziendale e il ripristino d'emergenza.	Un piano per il ripristino d'emergenza deve prevedere quanto segue: ▪ criteri definiti per determinare se un sistema è fondamentale per le attività del fornitore, ▪ elenco dei sistemi fondamentali redatto in base ai criteri definiti che devono essere oggetto del ripristino in caso di emergenza, ▪ procedura di ripristino d'emergenza definita per ogni sistema fondamentale che garantisca che un tecnico che non conosce il sistema possa ripristinare l'applicazione in meno di 72 ore, e

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione J - Sicurezza (continua)	
		▪ verifiche annuali (o più frequenti) e revisione dei piani di ripristino d'emergenza per garantire il raggiungimento degli obiettivi di ripristino.
46	Autenticazione dell'identità di una persona prima di concederle l'accesso ai dati personali o riservati di Microsoft e garanzia che l'accesso sia limitato all'ambito delle attività di tale specifica persona consentite a supporto della Prestazione.	Tutti gli ID utente devono essere univoci e va garantito che ciascuno disponga di un metodo di autenticazione standard del settore come Azure Active Directory. L'accesso a livelli superiori (amministrativo o altri tipi di privilegio avanzato) deve richiedere l'utilizzo di un secondo fattore di autenticazione, come una smart card o un autenticatore basato sul telefono. Un programma di sicurezza delle informazioni documentato che garantisca che l'accesso di tutti i dipendenti dei fornitori e dei subappaltatori ai dati personali o riservati di Microsoft non sia più esteso o duri più del necessario a supporto della Prestazione.
47	Il fornitore dovrà proteggere tutti i dati trattati che transitano nelle reti, in relazione alla sua Prestazione, mediante crittografia utilizzando Transport Layer Security ("**TLS**") o Internet Protocol Security ("**IPsec**"). Questi metodi sono descritti nel NIST 800-52 e nel NIST 800-57. Può essere utilizzato anche uno standard del settore equivalente. Il fornitore dovrà rifiutare la consegna di qualsiasi dato personale o riservato di Microsoft trasmesso tramite mezzi non crittografati.	Deve essere stabilito e attuato il processo di creazione, distribuzione e sostituzione di certificati TLS o altri.
48	Tutti i dispositivi del fornitore (laptop, postazioni di lavoro e così via) che verranno utilizzati per accedere o per gestire i dati personali o riservati di Microsoft, devono utilizzare la crittografia basata su disco.	Tutti i dispositivi devono essere crittografati per soddisfare BitLocker o un'altra soluzione equivalente di crittografia del disco per tutti i dispositivi client utilizzati per gestire i dati personali o riservati di Microsoft.
49	Devono essere presenti sistemi e procedure (che utilizzano gli attuali standard di settore come quello descritto nello standard **NIST 800-111**) per la crittografia a riposo (quando archiviati) di tutti i dati personali e/o riservati di Microsoft, esempi includono, ma non sono limitati a: ▪ dati delle credenziali (ad esempio il nome/password dell'utente)	Verificare che i dati personali e riservati di Microsoft siano crittografati a riposo.

#	Requisiti di protezione dei dati dei fornitori Microsoft	Prova di conformità
	Sezione J - Sicurezza (continua)	
	▪ dati dello strumento di pagamento (ad esempio i numeri di carta di credito e di conto bancario) ▪ dati personali relativi all'immigrazione ▪ dati del profilo medico (ad esempio i numeri di cartelle cliniche o indicatori o identificatori biometrici, come il DNA, le impronte digitali, le retine e le iridi degli occhi, i modelli vocali, i modelli facciali e le misurazioni della mano, utilizzati a fini dell'autenticazione) ▪ dati identificativi rilasciati dal governo (ad esempio i numeri di previdenza sociale o di patente di guida) ▪ dati appartenenti a clienti Microsoft (ad esempio i clienti di SharePoint, Office 365, OneDrive) ▪ materiale relativo a prodotti Microsoft non ancora annunciati ▪ data di nascita ▪ informazioni sui profili di minori ▪ dati geografici in tempo reale ▪ indirizzo personale fisico (non aziendale) ▪ numeri di telefono personali (non aziendali) ▪ religione ▪ opinioni politiche ▪ orientamento/preferenza sessuale ▪ risposte alle domande di sicurezza (ad esempio l'autenticazione multi fattore, il ripristino della password) ▪ nome da nubile della madre	
50	Anonimizzazione di tutti i dati personali Microsoft utilizzati in un ambiente di sviluppo o verifica.	I dati personali di Microsoft non devono essere utilizzati in ambienti di sviluppo o verifica; se non esistono alternative, tali dati saranno anonimizzati per prevenire l'identificazione degli interessati o il loro uso improprio. Nota: i dati anonimizzati non sono quelli pseudonimizzati. I dati anonimizzati sono dati che non si riferiscono a una persona fisica identificata o identificabile, in cui l'interessato dei dati personali non è o non è più identificabile.

Glossario

Il "**Rappresentante autorizzato**" è una persona che dispone del livello appropriato di autorità per firmare per conto della società. Questa persona ha le necessarie conoscenze in materia di privacy e sicurezza o ha consultato un esperto in materia prima di inviare la propria risposta a un'azione del programma SSPA. Inoltre, aggiungendo il proprio nominativo in un modulo SSPA, tale persona attesta di aver letto e compreso i DPR.

"**EUDPR**" indica il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla protezione delle persone fisiche relativamente al trattamento dei dati personali da parte delle istituzioni, degli enti, degli uffici e delle agenzie dell'Unione e sulla libera circolazione di tali dati, e abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

"**Freelancer**" indica le persone che svolgono attività o servizi su richiesta, che vengono ingaggiate tramite piattaforme digitali o altri mezzi.

"**GDPR"** indica il regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e sulla libera circolazione di tali dati, e abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

"**Requisiti di protezione dei dati sulla privacy**" indica il GDPR, l'EUDPR, le leggi locali sulla protezione dei dati della UE/SEE, il California Consumer Privacy Act, Codice civile della California § 1798.100 e segg. ("*CCPA*") (Legge sulla privacy dei clienti della California), il Data Protection Act 2018 del Regno Unito (Legge sulla protezione dei dati) e qualsiasi legge, regolamento e altri requisiti legali correlati o successivi applicabili nel Regno Unito; e qualsiasi legge, regolamento e altri requisiti legali applicabili relativi a (a) privacy e sicurezza dei dati; o (b) utilizzo, raccolta, conservazione, archiviazione, sicurezza, divulgazione, trasferimento, eliminazione e altri trattamenti di dati personali.

"**Clausole modello UE**" **e** "**Clausole contrattuali standard**" indicano (i) le clausole standard di protezione dei dati per il trasferimento di dati personali ai responsabili del trattamento stabiliti in Paesi terzi che non garantiscono un livello adeguato di protezione dei dati, come descritto nell'articolo 46 del GDPR e approvato dalla decisione della Commissione Europea (UE) 2021/914 del 4 giugno 2021; (ii) eventuali clausole contrattuali standard successive adottate da (a) la Commissione europea, (b) il Garante europeo della protezione dei dati e approvate dalla Commissione europea, (c) il Regno Unito ai sensi del General Federal Data Protection Act del Regno Unito, (d) la Svizzera ai sensi della legge federale svizzera sulla protezione dei dati, o (e) da un governo in una giurisdizione diversa dalla Svizzera, dal Regno Unito e dalle giurisdizioni che compongono l'Unione Europea / Spazio economico europeo in cui le clausole regolano il trasferimento internazionale di dati personali, devono essere integrate e vincolanti per il fornitore a partire dal giorno della loro adozione.

"Website Hosting" indica un servizio di hosting di siti web online che crea e/o gestisce siti web per conto di Microsoft sotto il dominio Microsoft, ovvero il fornitore che fornisce tutti i materiali e i servizi necessari per creare e gestire un sito e lo rende accessibile su internet. Il "fornitore di servizi di hosting di siti web" o "host di siti web" è il fornitore che mette a disposizione gli strumenti e i servizi necessari per la visualizzazione del sito web o della pagina web su internet, come i cookie o i web beacon per la pubblicità.