

Addendum relativo al trattamento dei dati (precedentemente Addendum SaaS)

Il presente Addendum relativo al trattamento dei dati ("Data Processing Addendum" o "DPA") è incorporato nell'accordo relativo al software e/o nell'accordo relativo ai servizi ("Accordo") tra il Fornitore e il Cliente per quanto riguarda l'acquisto di determinate licenze software SaaS e/o Servizi di manutenzione e/o servizi professionali (a fini del presente DPA di seguito denominati "Servizi") e fa parte di un contratto scritto (anche in formato elettronico) tra il Fornitore e il Cliente. Tutti i termini in maiuscolo non definiti nel presente documento avranno il significato stabilito nel Contratto.

1. **Definizioni.** I termini in maiuscolo non definiti nel contesto o nel Contratto avranno i significati loro assegnati di seguito:
 - a) "**Titolare del trattamento**" indica la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi con cui viene compiuto il Trattamento dei Dati personali.
 - b) "**Legge sulla protezione dei dati**" indica tutte le leggi e i regolamenti applicabili al trattamento dei Dati personali del cliente ai sensi del Contratto, inclusi, a seconda dei casi: (i) il California Consumer Privacy Act, come modificato dal California Privacy Rights Act, e qualsiasi regolamento vincolante promulgato ("**CCPA**"), (ii) il Regolamento generale sulla protezione dei dati personali (regolamento (UE) 2016/679) ("**GDPR dell'UE**" o "**GDPR**"), (iii) la Legge federale svizzera sulla protezione dei dati ("LPD"), (iv) il GDPR dell'UE secondo quanto applicato dal diritto di Inghilterra e Galles in virtù della sezione 3 dell'Unione Europea (Withdrawal) Act 2018 (il "**GDPR del Regno Unito**") e (v) lo UK Data Protection Act 2018; per ogni Legge sulla protezione dei dati, come viene di volta in volta aggiornata, modificata o sostituita.
 - c) "**Interessato**" indica la persona fisica identificata o identificabile a cui fanno riferimento i Dati personali del Cliente.
 - d) "**Dati personali**" indica informazioni relative a una persona fisica identificata o identificabile o che rappresentano in altro modo "dati personali", "informazioni personali", "informazioni di identificazione personale" o termini simili secondo quanto definito nelle Leggi sulla protezione dei dati.
 - e) "**Violazione dei dati personali**" indica una distruzione, perdita o alterazione accidentale o illecita nonché una divulgazione non autorizzata o un accesso non autorizzato di terzi ai Dati personali del cliente trattati dal Fornitore. Qualora si verificasse tale violazione, il Titolare del trattamento è tenuto a comunicarla, ai sensi della Legge sulla protezione dei dati, agli Interessati o alle autorità di protezione dei dati competenti.
 - f) Per "**Trattamento**" si intende qualsiasi operazione eseguita su Dati personali, con o senza mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'utilizzo, la divulgazione mediante trasmissione, la diffusione o la disponibilità, l'allineamento o la combinazione, la restrizione, la cancellazione o la distruzione.
 - g) "**Responsabile del trattamento**" indica una persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che elabora i Dati personali per conto del Titolare del trattamento.
 - h) "**Clausole contrattuali standard**" o "**UE SCCs**" indica le Clausole contrattuali standard approvate dalla Commissione europea con la decisione 2021/914.
 - i) "**Sub-Responsabile del trattamento**" indica le Società affiliate del Fornitore e le terze parti ingaggiate dal Fornitore (o dalle Società affiliate del Fornitore) per quanto riguarda la fornitura di una parte o tutti i Servizi. Detti Sub-Responsabili del trattamento sono inoltre incaricati dell'elaborazione dei Dati personali del Cliente in conformità al presente DPA.

2. Trattamento dei Dati personali del cliente

Il Fornitore può trattare i Dati personali del Cliente nell'ambito dell'Accordo in qualità di Responsabile del trattamento, che agisce per conto del Cliente, in qualità di Titolare del trattamento (ovvero, a seconda dei casi, il Fornitore potrebbe agire in qualità di sub-responsabile del trattamento, per conto del Cliente, laddove quest'ultimo interviene in qualità di Responsabile del trattamento). Il Fornitore si impegna a trattare i Dati personali al solo scopo di adempiere ai propri obblighi nei confronti del Cliente ai sensi di e in conformità con (i) il presente DPA e il Contratto e (ii) le istruzioni scritte del Cliente o (iii) al fine di rispettare i propri obblighi ai sensi delle leggi applicabili, essendo inoltre soggetto a qualsiasi obbligo di notifica ai sensi delle Leggi sulla protezione dei dati. I dettagli relativi all'oggetto del trattamento, la relativa durata, natura, lo scopo nonché al tipo di Dati personali del Cliente e ai Interessati sono specificati nel Contratto o, se non fosse il caso, sono essere indicati nell'Allegato 1 del Appendice al presente DPA. Il Cliente e il Fornitore accettano di adempiere ai propri obblighi ai sensi delle Leggi sulla protezione dei dati applicabili ai Dati personali trattati in relazione ai Servizi. Il Cliente è l'unico responsabile del proprio rispetto delle Leggi sulla protezione dei dati relative al Trattamento dei Dati personali prima della divulgazione, il trasferimento o la messa a disposizione in qualsiasi modo dei Dati personali al Fornitore. Il Fornitore informerà immediatamente il Cliente qualora, a suo avviso, le istruzioni risultino in violazione delle Leggi sulla protezione dei dati.

3. Sicurezza del trattamento

- a) **Politiche generali di sicurezza.** Il Fornitore metterà in pratica e manterrà misure, procedure e pratiche tecniche e organizzative, in base alla natura dei Dati personali del Cliente, elaborate per proteggere la sicurezza, la riservatezza, l'integrità e la disponibilità dei Dati personali del Cliente nonché per proteggere tali dati da eventuali Violazioni dei dati personali, in conformità con le misure di sicurezza del Fornitore a cui si fa riferimento nell'Accordo e come ulteriormente descritto all'indirizzo: <https://www.oneidentity.com/legal/security.aspx> (collettivamente "**Sito per la sicurezza**"), tra cui è incluso quanto segue:
 - Politica di sicurezza delle informazioni,
 - Dichiarazione relativa alle misure tecniche e organizzative,
 - Politica di risposta alla Violazione dei dati personali e
 - Informativa sulla privacy.Il Cliente accetta che il Fornitore possa modificare il proprio Sito per la sicurezza, purché non riduca sostanzialmente il livello complessivo di protezione fornito.
- b) **Riservatezza.** Il Fornitore proteggerà i Dati personali del Cliente in conformità ai propri obblighi di riservatezza secondo quanto stabilito nel Contratto. Il Fornitore garantirà che il personale addetto al Trattamento dei Dati personali del Cliente abbia stipulato accordi di riservatezza per iscritto con il Fornitore. Il Fornitore garantirà che tali obblighi di riservatezza

sopravvivano alla risoluzione del rapporto lavorativo relativamente a detto personale. Il Fornitore formerà adeguatamente il personale avente accesso ai Dati personali del Cliente sui requisiti e sui principi di sicurezza e privacy dei dati.

4. Richieste degli Interessati.

Su richiesta del Cliente, il Fornitore collaborerà ragionevolmente per aiutare il Cliente a rispettare gli obblighi del Cliente ai sensi delle Leggi sulla protezione dei dati di rispondere alle richieste presentate dai diversi soggetti relative all'esercizio dei propri diritti ai sensi delle Leggi sulla protezione dei dati, qualora il Cliente non potesse ragionevolmente soddisfare tali richieste in modo indipendente (anche attraverso l'uso dei Servizi). Qualora il Fornitore riceva una richiesta da parte dell'Interessato relativamente ai Dati personali trattati ai sensi del presente documento, il Fornitore consiglierà all'Interessato (qualora quest'ultimo abbia fornito informazioni volte a identificare il Cliente) di reindirizzare la sua richiesta al Cliente.

5. Diritto di audit.

- a) **Registri generali del Fornitore.** Il Fornitore conserverà determinati registri relativi al Trattamento svolto in conformità con le Leggi sulla protezione dei dati e, su richiesta scritta da parte del Cliente, metterà a disposizione del Cliente qualsiasi registro ragionevolmente necessario per dimostrare la conformità agli obblighi del Fornitore ai sensi del presente DPA e delle Leggi sulla protezione dei dati applicabili.
- b) **Programma di conformità di terze parti.** Il Fornitore descriverà gli eventuali propri programmi di audite e certificazione di terze parti e, su richiesta scritta da parte del Cliente (nel rispetto degli obblighi di riservatezza stabiliti nell'Accordo), metterà a disposizione del Cliente copie riassuntive dei propri rapporti di audit (ciascuno, un "Rapporto di Audit"). Il Cliente potrà condividere una copia dei Rapporti di Audit con le autorità governative competenti, se necessario.
- c) **Audit del cliente.** Il Cliente potrà, a proprie spese, condurre un audit in base a un piano concordato di comune accordo con il Fornitore che sia coerente con i parametri dell'audit riportati di seguito (un "Audit"). Il Cliente potrà esercitare i propri diritti di audit (1) qualora la fornitura di un Rapporto di Audit da parte del Fornitore fornisca informazioni insufficienti, le quali non consentono al Cliente di verificare la conformità del Fornitore al presente DPA o la conformità alle Leggi sulla protezione dei dati; o (2) qualora tale rapporto fosse necessario per consentire al Cliente di rispondere a un'audit da parte di un'autorità governativa o (3) in relazione a una Violazione dei dati personali.
Ogni Audit dovrà (1) essere condotto da una terza parte indipendente che abbia stipulato un accordo di riservatezza con il Fornitore, (2) essere limitato a quanto ragionevolmente richiesto al Cliente al fine di valutare la conformità del Fornitore al presente DPA e la conformità delle parti alle Leggi sulla protezione dei dati, (3) avere luogo in una data e in un'ora concordate mutualmente e solo durante il normale orario lavorativo del Fornitore, (4) non avere luogo più di una volta all'anno (fatto salvo nel caso in cui sia espressamente richiesto dalle Leggi sulla protezione dei dati o in relazione a una Violazione dei dati personali), (5) limitarsi alle infrastrutture controllate direttamente dal Fornitore, (6) limitare i risultati ai soli Dati personali del Cliente e (7) trattare i risultati come informazioni riservate nei limiti massimi consentiti dalle Leggi sulla protezione dei dati.

6. Sub-Responsabili del trattamento e Trasferimenti internazionali.

- a) **Utilizzo di Sub-responsabili del trattamento.** Il Cliente autorizza generalmente il Fornitore a coinvolgere diversi Sub-responsabili del trattamento in relazione alla fornitura dei Servizi. Il Fornitore stipulerà accordi scritti appropriati con i Sub-responsabili del trattamento in conformità alle disposizioni del presente DPA e alle istruzioni tra il Cliente e il Fornitore contenute nel presente documento. Il Fornitore sarà responsabile da ogni violazione del presente DPA nella misura in cui tale violazione venga causata da Sub-Responsabili del trattamento assunti dal Fornitore.
- b) **Elenco dei Sub-responsabili del trattamento.** Il Fornitore conserva gli elenchi dei Sub-esponsabili del trattamento per ogni Prodotto software, incluse le loro funzioni e localizzazione, e li mette a disposizione del Cliente tramite la registrazione al sito <https://support.oneidentity.com/subprocessor>. Almeno trenta (30) giorni prima di autorizzare qualsiasi nuovo Sub-responsabile del trattamento ad accedere ai Dati personali, il Fornitore aggiornerà l'elenco dei Sub-responsabili del trattamento e informerà il Cliente tramite e-mail al momento della registrazione.
- c) **Obiezioni relative ai nuovi Sub-responsabili del trattamento.** Qualora il Cliente non approvi un nuovo Sub-responsabile del trattamento, quest'ultimo potrà rescindere qualsiasi abbonamento relativo al Software SaaS applicabile, inviando, prima del termine del periodo di preavviso, una notifica scritta di richiesta di risoluzione che includa una spiegazione dei motivi per cui non approva i nuovi Sub-responsabili del trattamento.
- d) **Trasferimenti internazionali.** Per il trasferimento di Dati personali europei e/o del Regno Unito a un Sub-responsabile del trattamento situato in un paese terzo che non fornisce un'adeguata protezione dei Dati personali, il Fornitore e il relativo Sub-responsabile del trattamento dovranno stipulare le Clausole contrattuali standard al fine di fornire tutele adeguate relative al trasferimento di tali Dati personali in conformità alle Leggi sulla protezione dei dati applicabile nell'Unione Europea e in Gran Bretagna.

7. Notifica di Violazione dei dati personali.

In aggiunta agli obblighi stabiliti nel Sito sulla Sicurezza, il Fornitore dovrà informare prontamente il Cliente non appena sia venuto a conoscenza di qualsiasi Violazione dei dati personali e dovrà fornire informazioni ragionevoli in suo possesso per aiutare il Cliente ad adempiere ai propri obblighi di segnalazione di una Violazione dei dati personali come richiesto dalle Leggi in materia di protezione dei dati. Il Fornitore può fornire tali informazioni in differenti momenti non appena diventano disponibili. Il Fornitore si impegna a compiere sforzi in buona fede per identificare la causa di tale Violazione dei Dati personali e ad adottare le misure che il Fornitore riterrà necessarie e ragionevoli al fine di porre rimedio alla causa della violazione nella misura in cui ciò sia sotto il suo ragionevole controllo

8. Cancellazione dei Dati personali del cliente.

Salvo il Cliente informi il Fornitore almeno trenta (30) giorni prima del completamento dei Servizi, in seguito alla risoluzione o alla scadenza del Contratto, il Fornitore eliminerà tutti i Dati personali del Cliente dai propri sistemi. Il Fornitore eseguirà detta cancellazione nel rispetto delle pratiche standard sicure del settore in materia di cancellazione di dati. Indipendentemente da quanto sopra riportato, il Fornitore potrà conservare i Dati personali del Cliente: (i) secondo quanto previsto dalle Leggi sulla protezione dei dati o (ii) conformemente alle proprie politiche standard di backup o conservazione delle informazioni, a

condizione che, in entrambi i casi, il Fornitore (1) mantenga la riservatezza di, o rispetti in altro modo, le disposizioni applicabili del presente DPA per quanto riguarda i Dati personali conservati del Cliente e (2) non ci siano trattamenti ulteriori dei Dati personali conservati del Cliente, salvo per casi e durate specifici previsti nelle Leggi sulla protezione dei dati applicabili.

9. Valutazione dell'impatto sulla protezione dei dati.

Il Fornitore fornirà al Cliente la ragionevole cooperazione e assistenza necessarie per consentire al Cliente di adempiere ai suoi obblighi delle Leggi sulla protezione dei dati di effettuare una valutazione d'impatto sulla protezione dei dati o una valutazione del rischio simile relativa all'utilizzo dei Servizi da parte del Cliente.

APPENDICE AL DPA

La presente Appendice fa parte del DPA.

ALLEGATO I – Oggetto e natura del Trattamento

A. ELENCO DELLE PARTI

L'Accordo tra il Cliente in qualità di Titolare del trattamento e il Fornitore in qualità di Responsabile del trattamento contiene una descrizione di tutte le informazioni richieste, quali:

- nome, indirizzo, nome del referente,
- posizione e dettagli del contatto,
- attività relative ai dati trasferiti ai sensi delle presenti Clausole, e
- firma e data.

B. DESCRIZIONE DEL TRATTAMENTO

1. Categorie di Interessati i cui dati personali sono oggetto di trattamento

Salvo diversa disposizione da parte del Cliente, i Dati personali trattati si riferiscono alle seguenti categorie di Interessati:

- dipendenti, appaltatori, partner commerciali del Cliente.

2. Categorie di Dati personali trattati

Il Cliente determina le categorie di dati relative al proprio utilizzo dei Servizi. I Dati personali trattati riguardano tipicamente le seguenti categorie di dati:

- dettagli relativi all'impiego (che possono includere nome e indirizzo dell'azienda, titolo professionale, grado, dati demografici e relativi alla posizione) ricollegabili ai dipendenti del Cliente o ad altre terze parti le cui informazioni personali sono fornite da o per conto del Cliente;
- informazioni di sistema relative ai sistemi del Cliente, ai sistemi che il Cliente fornisce al Fornitore e ai Servizi acquistati ai sensi del Contratto nonché necessarie per la fornitura dei Servizi (tra cui figurano ID utente e password, nome del computer e dominio, indirizzo IP, numero GUID (identificatore unico globale) o ubicazione del computer o di un altro dispositivo utilizzato).

I Dati personali dei clienti trattati ai sensi del presente documento possono essere ricollegabili a partner commerciali passati, presenti e potenziali o ad altri soggetti collegati a tali partner commerciali.

3. Dati sensibili trattati (se applicabile)

Le categorie speciali di dati personali (dati sensibili) non devono essere fornite dal Cliente, a meno che non vengano identificate caso per caso e solo nella misura in cui le parti concordano che tali categorie speciali di dati debbano essere coperte dalla fornitura dei Servizi.

4. Frequenza del trattamento (ad esempio se i dati sono trattati un'unica volta o in modo continuo)

In modo continuo per l'intera durata di utilizzo dei Servizi.

5. Natura del trattamento

- a) In relazione ai Servizi di manutenzione: il Fornitore o i suoi Sub-Responsabili del trattamento forniranno assistenza qualora un Cliente dovesse inviare un ticket di richiesta di assistenza relativo a una mancata disponibilità o a un funzionamento difettoso del Software. Gli incaricati risponderanno alle telefonate e potranno svolgere interventi risolutivi relativi a problematiche di base. Inoltre, avranno la possibilità di gestire i ticket di assistenza grazie a un apposito sistema di tracciamento.
- b) In relazione ai servizi professionali: il Fornitore o i suoi Sub-Responsabili del trattamento Responsabili secondari forniranno i Servizi in oggetto nell'Ordine dei servizi.
- c) in relazione al Software SaaS: fornitura del Software SaaS sottoscritto dal Cliente.

6. Obiettivi del trasferimento dei dati e dell'ulteriore Trattamento

I Dati personali del Cliente trattati dal Fornitore saranno soggetti alle seguenti attività di trattamento di base:

- a) utilizzo dei Dati personali per consentire la fornitura dei Servizi e, ove applicabile, per fornire l'accesso e i vantaggi relativi al Software SaaS ai sensi del Contratto nonché per garantire assistenza tecnica su richiesta del Cliente e in conformità con i requisiti specifici del Cliente, a seconda dei casi, il tutto conformemente alle istruzioni descritte di seguito;
- b) conservazione dei Dati personali;
- c) trattamento informatico di Dati personali per la trasmissione di detti dati;
- d) miglioramento continuo delle caratteristiche e delle funzionalità del servizio fornite nell'ambito dei Servizi del Fornitore, tra cui automazione, elaborazione delle transazioni e apprendimento automatico;
- e) esecuzione delle istruzioni del Cliente conformemente al Contratto.

Le seguenti attività di Trattamento addizionali si applicano a tutti i Dati personali archiviati nel Software SaaS:

- a) conservazione dei Dati personali all'interno di data center (architettura multi-tenant);
- b) backup e ripristino dei Dati personali del cliente archiviati nel software SaaS;
- c) trattamento informatico dei dati personali, inclusa la trasmissione dei dati, il recupero dei dati, l'accesso ai dati;

- d) comunicazione agli utenti del Cliente;
- e) rilascio, sviluppo e caricamento di eventuali correzioni o aggiornamenti del Software SaaS;
- f) accesso alla rete per consentire il Trasferimento dei Dati personali;
- g) monitoraggio, risoluzione dei problemi e amministrazione dell'infrastruttura e della banca dati del Software SaaS sottostante;
- h) monitoraggio della sicurezza, rilevamento delle intrusioni basata sulla rete (network) e prove di penetrazione e,
- i) se necessario, attività di risposta e reindirizzamento delle richieste e dei Soggetti interessati in modo appropriato e conformemente alle istruzioni descritte qui di seguito.

Il Fornitore può utilizzare dati resi anonimi (che non sono Dati personali del Cliente ma possono essere derivati dagli stessi) correlati al miglioramento dei prodotti e allo sviluppo di nuovi prodotti e servizi del Fornitore .

Ulteriori dettagli su ciò che il Software SaaS fa, su come gestisce i Dati personali e sulla localizzazione dell'archiviazione dei dati sono indicati nella Documentazione del prodotto applicabile e nella Guida sulla sicurezza.

7. Il periodo di conservazione dei Dati personali previsto oppure, qualora ciò non fosse possibile, i criteri utilizzati per determinare tale periodo

I Dati personali saranno trattati durante l'utilizzo dei Servizi da parte del Cliente ai sensi del Contratto e nel rispetto della Sezione 8 del presente DPA.

8. Per quanto riguarda i trasferimenti a Sub-Responsabili del trattamento , è necessario specificare anche l'oggetto, la natura e la durata del Trattamento

Per quanto riguarda le Clausole contrattuali standard, i trasferimenti ai Sub-Responsabili del trattamento avverranno sulla stessa base di cui al presente DPA.

9. Istruzioni, impegni del Cliente e del Fornitore.

Il Fornitore seguirà le istruzioni scritte e documentate ricevute dal Cliente in relazione ai Dati personali del Cliente salvo che, a giudizio del Fornitore, tali istruzioni (1) siano illecite o possano comportare una violazione delle Leggi di protezione dei dati applicabili, (2) richiedano modifiche sostanziali al Software SaaS del Fornitore e/o (3) siano incompatibili con i termini del Contratto o della Documentazione del Fornitore relativa ai Servizi venduti nell'ambito del Contratto. In tali circostanze, il Fornitore dovrà informare immediatamente il Cliente del fatto che non può rispettare tali istruzioni. Qualsiasi descrizione relativa al Trattamento presente all'interno del Contratto, del DPA e di qualsiasi Documentazione correlata del Fornitore deve essere considerata come un'istruzione fornita dal Cliente.

ALLEGATO II - Dichiarazione relativa alle misure tecniche e organizzative.

Il Fornitore adotterà le misure tecniche e organizzative appropriate riportate nel Sito per la sicurezza (secondo quanto definito nella Sezione 3(a) del DPA) per quanto riguarda il Trattamento dei dati personali del Cliente indicato nel presente documento. Il Cliente accetta che il Fornitore possa modificare le misure adottate per proteggere i Dati personali del Cliente, purché ciò non riduca in modo sostanziale il livello generale di protezione dei dati concordato nel presente documento.