TRATTAMENTO DEI DATI PERSONALI PER I SERVIZI SAP CLOUD

(Personal Data Processing Agreement for SAP Cloud Services)

1. CONTESTO

1.1 Finalità e ambito di applicazione. Il presente documento ("**DPA**") è parte integrante del Contratto e costituisce un accordo scritto (anche in formato elettronico) tra SAP e il Cliente. Il presente DPA si applica ai Dati Personali trattati da SAP e dai suoi Sub-responsabili (Subprocessors) nell'ambito del Cloud Service. Il presente DPA non si applica agli ambienti non produttivi del Cloud Service qualora questi siano messi a disposizione da SAP e il Cliente non dovrà archiviare Dati Personali in tali ambienti.

1.2 Struttura. Le Appendici 1 e 2 formano parte integrante del presente DPA. Esse stabiliscono l'oggetto, la natura e le finalità del trattamento, la tipologia di Dati Personali, le categorie di soggetti interessati e le misure tecnico-organizzative applicabili.

1.3 GDPR. SAP e il Cliente concordano che ciascuna parte è tenuta a esaminare e adottare gli obblighi imposti ai Titolari e ai Responsabili dal Regolamento Generale sulla Protezione dei Dati 2016/679 ("**GDPR**"), in particolare gli Articoli 28 e 32 al 36 del GDPR, nell'ipotesi e nella misura applicabile ai Dati Personali del Cliente/Titolari che sono trattati nell'ambito del DPA. A fini illustrativi, l'Appendice 3 fornisce un elenco degli obblighi GDPR rilevanti e le sezioni corrispondenti del presente DPA.

1.4 Governance. SAP agisce in qualità di Responsabile mentre il Cliente e i soggetti che sono autorizzati ad usare il Cloud Service agiscono in qualità di Titolari ai sensi del DPA. Il Cliente è il punto di contatto univoco ed è il solo responsabile per l'ottenimento di tutte le eventuali autorizzazioni, consensi e permessi necessari per il trattamento dei Dati Personali ai sensi del presente DPA, inclusa l'approvazione dei Titolari ad usare SAP quale Responsabile ove necessario. Le autorizzazioni, consensi o permessi forniti dal Cliente, si intendono rilasciati non solo per conto del Cliente ma anche per conto di eventuali altri Titolari che utilizzano il Cloud Service. Nel caso in cui SAP informi o notifichi il Cliente, tale informazione o notifica verrà considerata ricevuta dai Titolari a cui il Cliente ha concesso l'utilizzo del Cloud Service ed è responsabilità del Cliente inoltrare tali informazioni e notifiche ai relativi Titolari.

2. SICUREZZA DEL TRATTAMENTO

2.1 Misure Tecniche e organizzative idonee. SAP ha implementato e applicherà le misure tecniche ed organizzative descritte nell'Appendice 2. Il Cliente ha esaminato tali misure e ritiene che le stesse sono appropriate per il Cloud Service selezionato nel Modulo d'Ordine tenendo conto dello stato dell'arte, dei costi di implementazione, della natura, ambito, contesto e finalità del trattamento dei Dati Personali.

2.2 Modifiche. SAP applica le misure tecnico-organizzative descritte all'Appendice 2 per l'intera base clienti SAP ospitati sul medesimo Data Center e che ricevono il medesimo Cloud Service. SAP potrà modificare le misure indicate all'Appendice 2 in qualsiasi momento e senza preavviso purché il livello di sicurezza adottato sia comparabile o migliore. Singole misure possono essere sostituite da nuove misure che sono finalizzate al medesimo scopo senza diminuire il livello di sicurezza posto a protezione dei Dati Personali.

3. OBBLIGHI IN CAPO A SAP

3.1 Istruzioni del Cliente. SAP tratterà i Dati Personali solo in conformità alle istruzioni documentate del Cliente. Il Contratto (incluso il presente DPA) rappresenta tali iniziali istruzioni documentate e l'utilizzo di ciascun Cloud Service si intende come istruzioni ulteriori. SAP farà quanto ragionevolmente possibile per implementare le eventuali ulteriori istruzioni del Cliente, sempre che siano richieste dalla Normativa sulla Protezione dei Dati, tecnicamente fattibili e non richiedano modifiche al Cloud Service. Ove una delle precedenti eccezioni sia applicabile, oppure se SAP non possa altrimenti attenersi ad una istruzione o ritenga che un'istruzione comporti una violazione della Normativa sulla Protezione dei Dati, SAP provvederà a darne comunicazione immediata al Cliente (anche tramite email).

3.2 **Trattamento imposto dalla legge.** SAP potrà trattare i Dati Personali anche nel caso sia richiesto dalla normativa applicabile. In tal caso, SAP informerà il Cliente di tale necessità prima del trattamento fatto, salvo il caso in cui la legge vieti la condivisione di tali informazioni per ragioni di interesse pubblico.

3.3 **Personale.** Per il trattamento dei Dati Personali, SAP e i Sub-responsabili concederanno l'accesso solo a persone autorizzate soggette all'obbligo di riservatezza. SAP e i Sub-responsabili formeranno regolarmente il personale che ha accesso ai Dati Personali sulle applicabili misure di sicurezza e di riservatezza dei dati.

3.4 **Cooperazione.** A richiesta del Cliente, SAP collaborerà ragionevolmente con il Cliente e i Titolari nella gestione delle richieste provenienti da Soggetti Interessati o autorità riguardo al trattamento dei Dati Personali da parte di SAP o eventuali Violazioni dei Dati Personali. SAP comunicherà al Cliente, non appena sia ragionevolmente possibile, eventuali richieste ricevute da un Soggetto Interessato in relazione al trattamento dei Dati Personali senza rispondere essa stessa a tale richiesta in mancanza di eventuali ulteriori istruzioni del Cliente. SAP fornirà le funzionalità che aiutano la correzione o rimozione da parte del Cliente dei Dati Personali dal Cloud Service, oppure limiterà il trattamento ai sensi della Normativa sulla Protezione dei Dati. Laddove tali funzionalità non vengano fornite, SAP provvederà a correggere o rimuovere eventuali Dati Personali, o a limitare il loro trattamento, secondo le istruzioni del Cliente e la Normativa sulla Protezione dei Dati.

3.5 **Notifica della Violazione dei Dati Personali.** Dopo esserne venuta a conoscenza, SAP informerà il Cliente senza ingiustificato ritardo di qualsiasi Violazione dei Dati Personali fornendo le ragionevoli informazioni in suo possesso al fine di aiutare il Cliente nell'adempimento dei suoi obblighi di segnalazione di una Violazione dei Dati Personali come richiesto dalla Normativa sulla Protezione dei Dati. SAP potrà fornire tali informazioni a fasi successive man mano che divengano disponibili. Tale comunicazione non potrà essere interpretata o intesa come un'ammissione di colpa o responsabilità da parte di SAP.

3.6 **Esame dell'Impatto della Protezione dei Dati.** Qualora, ai sensi della Normativa sulla Protezione dei Dati, il Cliente (o i suoi Titolari) sia tenuto a effettuare un esame sull'impatto della protezione dei dati oppure una preventiva consultazione con un'autorità, su richiesta del Cliente, SAP fornirà la documentazione che è generalmente disponibile per il Cloud Service (ad esempio, il presente DPA, il Contratto, relazioni di revisione o certificazioni). L'eventuale ulteriore supporto andrà concordato dalle Parti.

4. ESPORTAZIONE DEI DATI E CANCELLAZIONE

4.1 **Esportazione e recupero da parte del Cliente.** Nel corso del Periodo di Sottoscrizione e ai sensi del Contratto, il Cliente può accedere ai propri Dati Personali in ogni momento. Il Cliente potrà esportare e acquisire i propri Dati Personali in un formato standard. L'esportazione e l'acquisizione possono essere soggette a limitazioni tecniche, nel qual caso SAP e il Cliente faranno quanto ragionevolmente possibile per consentire al Cliente di accedere ai Dati Personali.

4.2 **Cancellazione.** Prima della scadenza del Periodo di Sottoscrizione, il Cliente potrà utilizzare gli strumenti di esportazione self-service di SAP (quali disponibili) per eseguire una migrazione finale dei Dati Personali dal Cloud Service (che si intenderà la "restituzione" dei Dati Personali). Il Cliente sin d'ora richiede a SAP di cancellare, al termine del Periodo di Sottoscrizione, i Dati Personali rimanenti sui server che ospitano il Cloud Service entro un ragionevole periodo di tempo in linea con la Normativa sulla Protezione dei Dati (che non potrà eccedere i sei mesi), fatto salvo che la normativa applicabile richieda la loro conservazione.

5. CERTIFICAZIONI E AUDIT

5.1 **Verifiche del Cliente.** Il Cliente o il suo auditor terzo indipendente che sia ragionevolmente accettabile da SAP (che non potranno comunque essere auditor terzi concorrenti di SAP o che non siano debitamente qualificati o indipendenti) potranno verificare l'ambiente di controllo e le pratiche di sicurezza di SAP relative ai Dati Personali trattati da SAP solamente se:

(a) SAP non abbia fornito sufficiente evidenza della sua conformità con le misure tecniche ed organizzative che proteggono i sistemi produttivi del Cloud Service a mezzo di: (i) una certificazione di conformità alla norma ISO 27001 o ad altri standard (l'ambito come definito nel certificato), oppure (ii) un valido ISAE3402 e/o ISAE3000 o altro attestato SOC1-3. Su richiesta del Cliente gli attestati delle verifiche o le certificazioni ISO sono disponibili tramite auditor terzi o tramite SAP;

(b) Si sia verificata una Violazione dei Dati personali;

(c) L'autorità di protezione dei dati del Titolare del Trattamento abbia presentato richiesta formale di verifica; oppure

(d) La Normativa obbligatoria sulla Protezione dei Dati Personali riconosca al Cliente il diritto per una verifica diretta, fatto salvo che il Cliente potrà effettuare la verifica una sola volta ogni dodici mesi a meno che la Normativa di legge sulla Protezione dei Dati richieda verifiche più frequenti.

5.2 Verifiche dell'altro Titolare. Eventuali altri Titolari potranno sottoporre a verifica l'ambiente di controllo e le procedure di sicurezza di SAP relative ai Dati Personali trattati da SAP ai sensi della Clausola 5.1 solamente se le ipotesi elencate nella medesima Clausola siano applicabili a tale diverso Titolare. Tale verifica dovrà essere effettuata dal Cliente come stabilito alla Clausola 5.1 a meno che la verifica non debba essere effettuata dall'altro Titolare ai sensi della Normativa sulla Protezione dei Dati. Nel caso in cui diversi Titolari i cui Dati Personali vengano trattati da SAP ai sensi del Contratto richiedano una verifica, il Cliente dovrà utilizzare tutti i mezzi ragionevoli per combinare le verifiche ed evitare verifiche multiple.

5.3 Ambito della verifica. Il Cliente dovrà dare un preavviso di almeno sessanta giorni per qualsiasi verifica, a meno che la Normativa sulla Protezione dei Dati o un'autorità della protezione dei dati competente richieda un preavviso più breve. La frequenza e l'ambito di qualsiasi verifica andrà concordata dalle parti che agiranno ragionevolmente e in buona fede. Le verifiche dei Clienti non potranno superare tre giorni lavorativi. Oltre tali limitazioni, le parti utilizzeranno le certificazioni in vigore o le altre relazioni di verifica al fine di evitare o minimizzare la ripetizione delle verifiche. Il Cliente dovrà fornire a SAP i risultati di tutte le verifiche.

5.4 Costo delle Verifiche. Il Cliente dovrà sostenere i costi di qualsiasi verifica a meno che tale verifica evidenzi un grave inadempimento di SAP del presente DPA, in tal caso SAP sosterrà i costi della verifica a proprie spese. Qualora all'esito di una verifica risulti che SAP si sia resa inadempiente delle obbligazioni poste a suo carico ai sensi del DPA, SAP dovrà porre immediatamente rimedio all'inadempimento a proprie spese.

6. SUB-RESPONSABILI

6.1 Usi consentiti. A SAP viene concessa un'autorizzazione generale di affidare il trattamento dei Dati Personali a Sub-responsabili, a condizione che:

(a) SAP o SAP SE per suo conto nomineranno i Sub-responsabili ai sensi di un contratto scritto (anche in formato elettronico) che sia conforme con le disposizioni del presente DPA in relazione con il trattamento dei Dati Personali da parte del Sub-responsabile. SAP sarà responsabile per qualsiasi violazione del Sub-responsabile ai sensi del presente Contratto;

(b) SAP valuterà le procedure di sicurezza, privacy e riservatezza del Sub-responsabile prima della sua nomina per stabilire se esso sia in grado di garantire il livello di protezione dei Dati Personali imposto dal presente DPA; e

(c) La lista dei Sub-responsabili di SAP in vigore alla data di decorrenza del Contratto sia resa pubblica da SAP oppure messa a disposizione da SAP al Cliente a richiesta, ivi compreso il nominativo, l'indirizzo e la qualifica di ciascun Sub-responsabile utilizzato da SAP per fornire il Cloud Service.

6.2 Nuovi Sub-responsabili. L'utilizzo di Sub-responsabili da parte di SAP sarà effettuato a sua discrezione, a condizione che:

(a) SAP informi il Cliente in anticipo (a mezzo di email o pubblicando un messaggio sul portale del supporto accessibile mediante SAP Support) l'intenzione di aggiungere o sostituire

all'elenco Sub-responsabili ivi compreso il nominativo, l'indirizzo e la qualifica del nuovo Sub-responsabile; e

(b) il Cliente potrà opporsi a tali modifiche nei termini di cui alla Clausola 6.3.

6.3 Opposizione ai Nuovi Sub-responsabili.

(a) Qualora abbia un fondato motivo ai sensi della Normativa sulla Protezione dei Dati di opporsi al trattamento dei Dati Personali da parte dei nuovi Sub-responsabili, il Cliente potrà recedere dal Contratto (limitatamente ai Cloud Services per i quali si intenda impiegare il nuovo Sub-responsabile) dandone comunicazione scritta a SAP. Tale recesso avrà effetto alla data stabilita dal Cliente che non potrà essere superiore a trenta giorni dalla data della comunicazione inviata da SAP al Cliente, in cui lo si informi del nuovo Sub-responsabile. Nel caso in cui non receda dal Contratto entro tale termine di trenta giorni, si riterrà che il Cliente abbia accettato il nuovo Sub-responsabile.

(b) Entro il termine di trenta giorni dalla data della comunicazione di SAP in cui si informa il Cliente del nuovo Sub-responsabile, il Cliente potrà chiedere di discutere in buona fede con SAP l'obiezione. Tali discussioni non allungheranno il termine per il recesso e non inficeranno il diritto di SAP di utilizzare il nuovo Sub-responsabile successivamente il periodo di trenta giorni.

(c) L'eventuale recesso ai sensi della presente Clausola 6.3 andrà considerato essere senza colpa delle parti e sarà sottoposta ai termini del Contratto.

6.4 Sostituzione di Emergenza. SAP potrà sostituire un Sub-responsabile senza preavviso qualora la ragione per la sostituzione esuli dal ragionevole controllo di SAP e si renda necessaria una sostituzione tempestiva per ragioni di sicurezza o per altre ragioni urgenti. In tal caso, SAP provvederà al più presto ad informare il Cliente della sostituzione del Sub-responsabile successivamente alla sua nomina. La Clausola 6.3 si applicherà di conseguenza.

7. TRATTAMENTO INTERNAZIONALE

7.1 Condizioni per il Trattamento Internazionale. SAP potrà trattare i Dati Personali, anche con l'utilizzo di Sub-responsabili, ai sensi del presente DPA al di fuori del paese in cui abbia sede il Cliente nei limiti consentiti dalla Normativa sulla Protezione dei Dati.

7.2 Clausole Contrattuali Standard. Qualora (i) i Dati Personali di un Titolare situato nello SEE o in Svizzera siano trattati in uno stato al di fuori dallo SEE, dalla Svizzera e di qualunque altro paese, organizzazione o territorio riconosciuto dall'Unione Europea come paese sicuro con un livello adeguato di protezione dei dati ai sensi dell'art. 45 del GDPR, o quando (ii) i Dati Personali di un altro Titolare siano trattati a livello internazionale e tale trattamento internazionale richieda un livello di adeguatezza dei dati ai sensi delle norme dello stato del Titolare, l'adeguatezza richiesta può essere raggiunta con la stipulazione di Clausole Contrattuali Standard, allora:

(a) SAP e il Cliente adotteranno le Clausole Contrattuali Standard;

(b) Il Cliente applicherà le Clausole Contrattuali Standard con ciascun Sub-responsabile interessato con una le seguenti modalità (i) il Cliente potrà beneficiare delle Clausole Contrattuali Standard stipulate da SAP o SAP SE e il Sub-responsabile acquisendo i relativi diritti e obblighi ("Modello di Accessione") oppure (ii) il Sub-responsabile (rappresentato da SAP) sottoscrive le Clausole Contrattuali Standard con il Cliente ("Modello di Procura"). Il Modello di Procura si applicherà solo quando SAP abbia espressamente confermato che un Sub-responsabile è idoneo a beneficiarne tramite l'elenco dei Sub-responsabili prevista alla Clausola 6.1(c), ovvero tramite una comunicazione al Cliente; oppure

(c) Altri Titolari il cui utilizzo dei Cloud Services sia stato autorizzato dal Cliente ai sensi del Contratto possono altresì aderire alle Clausole Contrattuali Standard con SAP e/o con i relativi Sub-responsabili nella stessa modalità del Cliente ai sensi delle precedenti Clausole 7.2 (a) e 7.2 (b). In tal caso, il Cliente aderirà alle Clausole Contrattuali Standard per conto degli altri Titolari.

7.3 **Rapporto delle Clausole Contrattuali Standard con il Contratto.** In nessun caso il presente Contratto avrà prevalenza sulle Clausole Contrattuali Standard in caso di conflitto. Notabene, le disposizioni di cui alle precedenti Clausole 5 e 6 sui diritti di verifica e i Sub-responsabili si applicano anche in relazione alle Clausole Contrattuali Standard.

7.4 **Legge Applicabile alle Clausole Contrattuali Standard.** Le Clausole Contrattuali Standard sono disciplinate dalla legge del paese dove ha sede il Titolare.

8. DOCUMENTAZIONE; REGISTRI DI TRATTAMENTO

Ciascuna parte è tenuta ad osservare gli obblighi di documentazione posti a suo carico, in particolare con riferimento al mantenimento dei registri del trattamento quando sono richiesti dalla Normativa sul Trattamento dei Dati. Ciascuna parte fornirà la ragionevole assistenza all'altra con riguardo agli obblighi di documentazione, ivi compreso il rilascio delle informazioni che l'altra parte necessiti con la ragionevole modalità richiesta dall'altra parte (come ad esempio utilizzando un sistema elettronico) al fine di mettere l'altra parte nella condizione di rispettare tutti gli obblighi relativi al mantenimento dei registri del trattamento.

9. ACCESSO UE

9.1 **Servizio Opzionale.** L'Accesso UE è un servizio opzionale che può essere eventualmente offerto da SAP. SAP fornirà il Cloud Service ammissibile per l'Accesso UE solamente per le istanze di produzione ai sensi della presente Clausola 9. Nel caso in cui l'Accesso UE non sia esplicitamente indicato e concordato nel Modulo d'Ordine, la presente Clausola 9 non si applicherà.

9.2 **Accesso UE.** SAP utilizzerà solo Sub-responsabili che hanno sede in Europa per la fornitura del supporto che richiede l'accesso ai Dati Personali nel Cloud Service e SAP non esporterà i Dati Personali al di fuori del SEE o della Svizzera salvo espressa autorizzazione scritta del Cliente (le email sono ammesse) rilasciata caso per caso, o come escluso ai sensi della Clausola 9.4.

9.3 **Sedi dei Data Center.** Alla Data di Efficacia del Contratto, i Data Center utilizzati per ospitare i Dati Personali nel Cloud Service sono situati nello SEE ed in Svizzera. SAP non trasferirà l'istanza del Cliente in un Data Center ubicato al di fuori del SEE o Svizzera senza il suo previo consenso scritto (le email sono ammesse). Qualora SAP preveda di trasferire l'istanza del Cliente in un altro Data Center ubicato nello SEE o Svizzera, SAP ne darà comunicazione scritta al Cliente (le email sono ammesse) con almeno trenta giorni di preavviso sulla data prevista per la migrazione.

9.4 **Esclusioni.** I seguenti Dati Personali non sono soggetti alle previsioni di cui alle sezioni 9.2 e 9.3:

- **(a)** Informazioni di contatto del mittente di un ticket di supporto; e
- **(b)** Qualsiasi altro Dato Personale fornito dal Cliente nella compilazione di un ticket di supporto. Il Cliente può scegliere di non fornire i suddetti Dati Personali all'atto della compilazione del ticket di supporto. Se tali dati sono necessari al processo di gestione degli incidenti, il Cliente potrà rendere anonimi i Dati Personali prima di trasmettere il messaggio di incidente a SAP.

10. DEFINIZIONI

Le espressioni con la lettera maiuscola che non sono definite nel presente documento saranno da intendersi nel significato loro attribuito nel Contratto.

10.1 **"Titolare"** si riferisce alla persona fisica o giuridica, all'autorità pubblica, all'agenzia o ad altro ente che, da solo o con altri, determini le finalità e le modalità di trattamento dei Dati Personali; ai fini del presente DPA, quando il Cliente agisce da responsabile di un altro titolare, verso SAP sarà considerato in rapporto con SAP un Titolare supplementare ed indipendente con i rispettivi diritti ed obblighi del Titolare ai sensi del presente DPA.

10.2 **"Data Center"** si riferisce al luogo dove l'istanza in produzione del Cloud Service per il Cliente è ospitata, come pubblicato all'indirizzo: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html o notificato al Cliente o altrimenti concordato nel Modulo d'Ordine.

10.3 **"Normativa sulla Protezione dei Dati"** si riferisce alla normativa vigente posta a tutela dei diritti e delle libertà fondamentali delle persone in merito alla privacy con riguardo al trattamento dei Dati Personali ai sensi del Contratto (e comprende, per quanto concerne il rapporto tra le parti

relativo al trattamento dei Dati Personali effettuato da SAP per contro del Cliente, il GDPR come standard minimo, indipendentemente dal fatto che i Dati Personali siano o meno soggetti al GDPR).

10.4 **"Soggetto Interessato"** si riferisce ad una persona fisica identificata o identificabile quale definita dalla Normativa sulla Protezione dei Dati.

10.5 **"SEE"** si riferisce allo Spazio Economico Europeo, in particolare agli Stati Membri dell'Unione Europea unitamente all'Islanda, al Liechtenstein e alla Norvegia.

10.6 **"Sub-responsabile europeo"** si riferisce ad un Sub-responsabile che tratti fisicamente i Dati Personali nello SEE o in Svizzera.

10.7 **"Dati Personali"** si riferisce a qualunque informazione relativa ad un Soggetto Interessato che goda di protezione ai sensi della Normativa sulla Protezione dei Dati. Ai fini del DPA, essi comprendono solamente i dati personali che siano (i) inseriti dal Cliente o dai suoi Utenti Autorizzati o derivati dal loro utilizzo del Cloud Service o (ii) forniti a o a cui accede SAP o i suoi Sub-responsabili per fornire supporto ai sensi del Contratto. I Dati Personali rappresentano un sotto insieme dei Dati Clienti (quali definiti dal Contratto).

10.8 **"Violazione dei Dati Personali"** si riferisce ad una confermata (1) accidentale o illegittima distruzione, perdita, alterazione, divulgazione non autorizzata o accesso di terzi non autorizzato a Dati Personali, oppure (2) incidente simile che interessi i Dati Personali per i quali la normativa applicabile prevede per il Titolare l'obbligo di notifica alle autorità per la protezione dei dati competenti o ai Soggetti Interessati.

10.9 **"Responsabile"** si riferisce alla persona fisica o giuridica, all'autorità pubblica, agente o ad altro ente che tratta i dati personali per conto del titolare, sia direttamente quale responsabile di un titolare o indirettamente quale Sub-responsabile di un titolare che tratti dati personali per conto del titolare.

10.10 **"Clausole Contrattuali Standard",** denominate anche "Clausole Standard UE", si riferiscono alle Clausole Contrattuali Standard o altra versione successiva delle stesse pubblicate dalla Commissione Europea (che troveranno applicazione automatica).

10.11 **"Sub-responsabile"** si riferisce alle Affiliate di SAP, SAP SE, Affiliate di SAP SE e terzi incaricati da SAP, SAP SE o dalle Affiliate di SAP SE in relazione con il Cloud Service e che trattano i Dati Personali ai sensi del presente DPA.

Appendice 1 al DPA e, ove applicabili, alle Clausole Contrattuali Standard

Esportatore
L'Esportatore è il Cliente che ha sottoscritto il al Cloud Service che consente agli Utenti Autorizzati di acquisire, modificare, usare, eliminare o altrimenti trattare i Dati Personali. Nel caso in cui il Cliente permetta ai Titolari di utilizzare anche il Cloud Service, tali altri Titolari sono anche Esportatori.

Importatore
SAP e i suoi Sub-responsabili forniscono il Cloud Service che include anche il seguente supporto:

Le Affiliate SAP SE nel mondo mantengono i data center del Cloud Service in remoto dalle rispettive sedi, quali quelle di St. Leon/Rot (Germania), India, e altre sedi SAP di stanziamento del personale addetto alle attività operative e di fornitura in Cloud. Il supporto comprende:

- Monitoraggio del Cloud Service
- Backup e ripristino dei Dati Cliente custoditi nel Cloud Service
- Rilascio e sviluppo di riparazioni e upgrade del Cloud Service
- Monitoraggio, ricerca guasti e amministrazione della struttura e database Cloud Service sottostanti
- Monitoraggio di sicurezza, supporto in rete per la rilevazione di accessi non autorizzati, test di penetrazione

Le Affiliate SAP SE forniscono supporto quando il Cliente sottopone un ticket di assistenza perché il Cloud Service non è disponibile o non funziona come previsto per alcuni o per tutti gli Utenti Autorizzati. SAP risponde alle chiamate telefoniche ed effettua ricerche guasto di base, e gestisce i ticket di supporto in un sistema di tracciatura che è separato dall'istanza di produzione del Cloud Service.

Soggetti interessati
Salvo altrimenti disposto dall'Esportatore, i Dati Personali trasferiti si riferiscono alle seguenti categorie di Soggetti Interessati: dipendenti, terzisti, business partner o altri soggetti i cui Dati personali vengono archiviati nel Cloud Service.

Categorie di Dati
I Dati Personali trasferiti riguardano le seguenti categorie di dati:

Il Cliente determina le categorie di dati di ciascun Cloud Service sottoscritto. Il Cliente può configurare i campi dei dati durante l'implementazione del Cloud Service o come altrimenti previsto nel Cloud Service stesso. I Dati Personali trasferiti riguardano in genere le seguenti categorie di dati: nome, numeri di telefono, indirizzi di posta elettronica, fuso orario, indirizzo postale, dati relativi all'accesso o all'utilizzo del sistema o di autorizzazione, ragione sociale, dati contrattuali, dati di fatturazione e un qualsiasi dato specifico dell'applicazione acquisito nel Cloud Service dagli Utenti Autorizzati, e possono comprendere i dati riguardanti l'appoggio bancario, la carta di credito o la carta di debito.

Categorie Speciali di Dati (se applicabile)
I Dati Personali trasferiti riguardano le seguenti categorie particolari di dati: come eventualmente previsto dal Contratto (compreso il Modulo d'Ordine).

Operazioni / Finalità del Trattamento
I Dati Personali trasferiti sono sottoposti alle seguenti attività di trattamento di base:

- uso dei Dati Personali per configurare, fare funzionare, monitorare e erogare il Cloud Service (compreso il supporto operativo e tecnico)
- fornitura dei Servizi di Consulenza;
- comunicazione agli Utenti Autorizzati
- archiviazione dei Dati Personali in Data Center dedicati (con architettura multi-tenant)
- upload di eventuali riparazioni o upgrade del Cloud Service
- back up dei Dati Personali

- trattamento computerizzato dei Dati Personali, compresa la trasmissione, il reperimento e l'accesso ai dati
- accesso di rete per consentire il trasferimento dei Dati Personali
- l’esecuzione delle istruzioni del Cliente ai sensi del Contratto

Appendice 2 al DPA e, ove applicabili, alle Clausole Contrattuali Standard – Misure Tecnico-Organizzative

1. MISURE TECNICO-ORGANIZZATIVE

Le successive sezioni definiscono le attuali misure tecnico-organizzative di SAP. SAP si riserva il diritto di poterle modificare in un qualsiasi momento senza obbligo di preavviso e purché sia mantenuto un pari o superiore livello di sicurezza. Le misure individuali possono essere sostituite da nuove misure che siano finalizzate al medesimo scopo senza ridurre il livello di sicurezza posto a protezione dei Dati Personali.

1.1 Controllo dell'accesso fisico. Ai soggetti non autorizzati è negato l'accesso fisico ai luoghi, edifici o stanze di ubicazione dei sistemi di trattamento dei dati che trattano e/o fanno uso di Dati Personali.

Misure:

- SAP protegge i propri beni e strutture utilizzando i mezzi idonei basati sulla SAP Security Policy
- In genere, gli edifici sono messi in sicurezza tramite sistemi di accesso controllato (ad es. sistema di accesso con carte magnetiche).
- Come requisito di base, i punti di accesso più esterni dell'edificio devono essere equipaggiati con un sistema di chiavi certificate, comprendente un sistema di gestione delle chiavi moderno e proattivo.
- A seconda della classificazione di sicurezza, gli edifici, le singole aree e gli edifici limitrofi possono essere ulteriormente protetti con misure addizionali. Queste includono specifici profili di accesso, sorveglianza video, sistemi con dispositivi di sicurezza e sistemi di controllo dell'accesso a riconoscimento biometrico.
- I diritti di accesso sono conferiti ai soggetti autorizzati su base individuale in conformità delle misure di controllo dell'accesso al sistema e ai dati (vedi i punti 1.2 e 1.3 a seguire). Ciò vale anche per l'accesso dei visitatori. Ospiti e visitatori agli edifici SAP devono registrare il proprio nome alla reception ed essere accompagnati da personale autorizzato SAP.
- I dipendenti SAP e il personale esterno devono indossare le proprie tessere identificative in tutte le sedi SAP.

Misure supplementari per i Data Center:

- Tutti i Data Center sono sottoposti a rigorose procedure di sicurezza affidate a guardie, telecamere di sorveglianza, rilevatori di movimento, meccanismi di controllo degli accessi e altre misure dirette ad impedire che apparecchiature e Data Center risultino compromessi. L'accesso ai sistemi e alle infrastrutture dei Data Center è ristretto al solo personale autorizzato. A garanzia del loro buon funzionamento, le attrezzature fisiche di sicurezza (quali i sensori di movimento, le telecamere, ecc.) devono essere sottoposte a manutenzione regolare.
- SAP e tutti i provider terzi dei Data Center sono tenuti a tenere un registro dei nomi e dei tempi del personale autorizzato che accede alle aree private SAP all'interno dei Data Center.

1.2 Controllo dell'Accesso al Sistema. È necessario impedire che i sistemi di trattamento dei dati utilizzati per erogare il Cloud Service siano utilizzati senza le debite autorizzazioni.

Misure:

- Per concedere l'accesso ai sistemi sensibili, inclusi quelli di archiviazione e trattamento dei Dati Personali, vengono utilizzati livelli multipli di autorizzazione. Le autorizzazioni sono gestite mediante processi definiti ai sensi della SAP Security Policy.
- Tutto il personale accede ai sistemi SAP con un identificativo unico (ID utente).
- SAP ha messo a punto procedure atte a garantire che le modifiche di autorizzazione richieste siano implementate esclusivamente in osservanza della SAP Security Policy (ad esempio, nessuna concessione di diritti senza autorizzazione). Nel caso in cui il personale lasci l'azienda, i loro diritti di accesso sono revocati.
- Le direttive SAP in materia di password proibiscono la condivisione delle password, stabiliscono il blocco dell'azione qualora una password venga svelata e impongono il cambiamento periodico della

password e la modifica delle password iniziali. Ai fini dell'autenticazione vengono assegnati ID utente personalizzati. Tutte le password devono soddisfare i requisiti minimi previsti ed essere memorizzate in forma criptata. Nel caso di password di dominio, il sistema ne impone una modifica conforme ai requisiti per le password complesse ogni sei mesi. Tutti i computer sono dotati di screensaver protetto da password.

- La rete aziendale è protetta dalla rete pubblica tramite firewall.
- SAP utilizza software antivirus aggiornati in tutti i punti di accesso alla rete aziendale (per profili di posta elettronica) sui file server così come sulle postazioni di lavoro.
- È stata implementata una gestione dei patch di sicurezza, in modo da assicurare la disponibilità regolare e periodica degli aggiornamenti di sicurezza pertinenti. È garantito il completo accesso remoto alla rete aziendale SAP e l'infrastruttura critica è protetta da un rigoroso sistema di autenticazione.

1.3 Controllo dell'Accesso ai Dati. I soggetti autorizzati all'uso dei sistemi di trattamento dei dati avranno accesso ai soli Dati Personali di pertinenza e non potranno leggere, copiare, modificare o eliminare i Dati Personali se non debitamente autorizzati durante il trattamento, uso e archiviazione.

Misure:

- Gli orientamenti in materia di sicurezza dei dati di SAP prevedono che ai Dati Personali sia applicato almeno lo stesso livello di protezione previsto per i dati "riservati" secondo lo standard di classificazione dei dati SAP.
- L'accesso ai Dati Personali viene concesso solo a fronte di necessità. Il Personale ha accesso alle informazioni che necessitano per adempiere ai suoi compiti. SAP impiega modelli autorizzativi che documentano i processi di concessione e i ruoli assegnati a ciascun account. Tutti i Dati Cliente sono protetti ai sensi della SAP Security Policy.
- Tutti i server di produzioni operano nei Data Center o in stanze server sicure. Le misure di sicurezza a protezione delle applicazioni di trattamento dei Dati Personali sono sottoposte a regolari controlli. A tal fine SAP conduce controlli di sicurezza interni ed esterni e test di penetrazione sui sistemi informatici.
- SAP non permette l'installazione di software diverso da quello approvato da SAP.
- Una norma di sicurezza SAP disciplina le modalità di cancellazione o distruzione dei dati o dei supporti dati una volta che essi non sono più necessari.

1.4 Controllo della Trasmissione dei Dati. Fatto salvo quanto sia necessario alla fornitura del Cloud Service ai sensi del Contratto, si fa divieto di leggere, copiare, modificare o eliminare i Dati Personali durante il loro trasferimento, in assenza di una debita autorizzazione. Se i supporti dati sono trasportati fisicamente, SAP adotta opportune misure atte a garantire i livelli di servizio concordati (quali codifica, contenitori piombati e così via).

Misure:

- I Dati Personali in trasferimento sulle rete interne SAP sono protetti ai sensi della SAP Security Policy.
- Al trasferimento dei dati tra SAP e i suoi clienti, le misure di sicurezza adottate per la protezione dei Dati Personali trasferiti sono quelle vicendevolmente concordate e facenti parte integrante del relativo Contratto. Ciò vale per i trasferimenti dati fisici e per quelli su rete. In ogni caso, il Cliente si assume la responsabilità relativa ad eventuali trasferimenti di dati una volta che essi siano al di fuori dei sistemi sotto il controllo di SAP (es. Dati trasmessi al di fuori del firewall del Data Center SAP).

1.5 Controllo dell'Inserimento dei Dati. Si ammette l'esame retrospettivo ai fini di stabilire se e chi abbia, presso SAP, inserito, modificato o eliminato i Dati Personali dal sistema di trattamento dati

Misure:

- SAP limita l'accesso ai Dati Personali al solo personale autorizzato e solo nella misura necessaria all'espletamento delle loro mansioni.

- SAP ha implementato un sistema di registrazione delle operazioni di inserimento, modifica eliminazione o blocco dei Dati Personali da parte di SAP o dei suoi Sub-responsabili entro il Cloud Service nella misura tecnicamente possibile.

1.6 Controllo Job. I Dati Personali trattati su mandato (es. Dati Personali trattati per conto del cliente) vengono trattati unicamente in conformità del Contratto, nonché delle istruzioni impartite dal Cliente.

Misure:

- SAP utilizza controlli e procedure per monitorare l'osservanza dei contratti stipulati tra SAP e i suoi clienti, Sub-responsabili o altri prestatori di servizi.
- Gli orientamenti in materia di sicurezza dei dati di SAP prevedono che ai Dati Personali sia applicato almeno lo stesso livello di protezione previsto per i dati "riservati" secondo lo standard di classificazione dei dati SAP.
- Tutti i dipendenti e i Sub-responsabili contrattuali o altri fornitori di servizi a SAP sono vincolati per contratto al rispetto della riservatezza di tutte le informazioni sensibili, che comprendono i segreti commerciali dei clienti e dei partner SAP.

1.7 Controllo di disponibilità. I Dati Personali saranno protetti contro distruzione o perdita accidentale o non autorizzata.

Misure:

- SAP impiega regolari processi di backup per assicurare il ripristino dei sistemi fondamentali quando si renda necessario.
- SAP utilizza un'alimentazione elettrica ininterrotta (UPS, batterie, generatori, ecc.) per assicurare un approvvigionamento elettrico ininterrotto ai Data Center.
- SAP ha definito piani di emergenza per i processi fondamentali e può offrire strategie di disaster recovery per i Servizi fondamentali come ulteriormente stabilito nella Documentazione o incorporato nel Modulo d'Ordine per il relativo Cloud Service.
- Le procedure e i sistemi di emergenza sono sottoposti a regolari test.

1.8 Controllo di Compartimentazione dei Dati. I Dati Personali raccolti per scopi diversi possono essere trattati separatamente.

Misure:

- SAP utilizza le funzionalità tecniche del software acquistato (quali la multi-tenancy o le infrastrutture distinte di sistema) per realizzare la compartimentazione tra Dati Personali provenienti da più clienti.
- Il Cliente (compresi i suoi Titolari) può accedere solo ai suoi dati.
- Qualora i Dati Personali siano necessari per la gestione di una richiesta di assistenza proveniente dal Cliente i dati vengono assegnati a tale messaggio specifico e vengono utilizzati unicamente per elaborare tale messaggio; non si accede ai dati per elaborare alcun altro messaggio. Tali dati sono custoditi in sistemi di supporto dedicati.

1.9 Controllo di Integrità dei Dati. I Dati Personali resteranno intatti, completi e aggiornati durante le attività di trattamento:

Misure:

SAP ha messo in pratica una strategia di difesa multi-livello come protezione contro modifiche non autorizzate.

In particolare, SAP utilizza le seguenti misure per dare attuazione alle disposizioni relative ai controlli e alle misure di cui sopra. Nello specifico:

- Firewall;
- Centro di Monitoraggio di Sicurezza;
- Software Antivirus;
- Backup e ripristino;
- Test di penetrazione interno o esterno;
- regolari ispezioni esterne per confermare le misure di sicurezza.

Appendice 3 al DPA e, ove applicabili, alle Clausole Contrattuali Standard

La seguente tabella indica gli Articoli del GDPR e le corrispondenti condizioni del DPA per soli fini illustrativi.

Articolo del GDPR	**Sezione del DPA**	**Cliccare sul link per visualizzare la Clausola**
28(1)	2 e Appendice 2	Sicurezza del Trattamento e Appendice 2, Misure Tecnico-Organizzative.
28(2), 28(3) (d) e 28 (4)	6	SUB-RESPONSABILI
28 (3) frase 1	1.1 e Appendice 1, 1.2	Finalità e ambito di applicazione. Struttura.
28(3) (a) e 29	3.1 e 3.2	Istruzioni del Cliente Trattamento imposto dalla legge.
28(3) (b)	3.3	Personale.
28(3) (c) e 32	2 e Appendice 2	Sicurezza del Trattamento e Appendice 2, Misure Tecnico-Organizzative.
28(3) (e)	3.4	Cooperazione.
28(3) (f) e 32-36	2 e Appendice 2, 3.5, 3.6	Sicurezza del Trattamento e Appendice 2, Misure Tecnico-Organizzative. Notifica della Violazione dei Dati Personali. Accertamento dell'Impatto della Protezione dei Dati.
28(3) (g)	4	Esportazione dei Dati e Cancellazione
28(3) (h)	5	CERTIFICAZIONI E AUDIT
28 (4)	6	SUB-RESPONSABILI
30	8	Documentazione; Registri di trattamento
46(2) (c)	7.2	Clausole Contrattuali Standard.

Appendice 4
CLAUSOLE CONTRATTUALI STANDARD (Standard Contractual Clauses)[1]

La Clausole Contrattuali Standard richiamate nel presente DPA sono pubblicate sul seguente link https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32010D0087&from=EN.

[1] Ai sensi della Decisione della Commissione del 5 febbraio 2010 (2010/87/UE)