TRATTAMENTO DEI DATI PERSONALI PER I SERVIZI SAP SUPPORT E PROFESSIONAL

(Personal Data Processing Agreement for SAP Support and Professional Services)

1. CONTESTO

1.1 Scopi ed Applicazione. Il presente documento ("**DPA**") viene integrato nel Contratto e forma parte di un contratto scritto (anche in formato elettronico) tra SAP e il Cliente. Il presente DPA si applica ai Dati Personali forniti dal Cliente e da ciascun Titolare del Trattamento in relazione all'esecuzione di servizi SAP stabiliti nel relativo Contratto ("Servizio(i) SAP") al quale il presente DPA è allegato e che possono comprendere:

(a) Il SAP Support come definito nel Contratto di Licenza Software e Supporto; e/o

(b) I Servizi Professionali quali descritti nel contratto di servizio stipulato da SAP e il Cliente ("Contratto di Servizio").

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 dati, i 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 ed ai Responsabili dal Regolamento Generale sulla Protezione dei Dati 2016/679 ("**GDPR**"), con particolare riguardo per gli Articoli 28 e 32 al 36 del GDPR, nell'ipotesi e nella misura applicabile ai Dati Personali del Cliente/Titolari che vengono trattati ai sensi 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 del Trattamento mentre il Cliente e i soggetti a cui permette di inserire Dati Personali nei sistemi accessibili da SAP nel corso dell'esecuzione del Servizio SAP agiscono in qualità di Titolari del Trattamento ai sensi del DPA. Il Cliente è il punto di contatto univoco ed è il solo responsabile per l'ottenimento di tutte le autorizzazioni, consensi e permessi necessari per il trattamento dei Dati Personali ai sensi del presente DPA, inclusa l'approvazione dei Clienti 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. 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 di inserire i Dati Personali ed è responsabilità del Cliente inoltrare tali informazioni ed avvisi ai relativi Titolari.

2. SICUREZZA DEL TRATTAMENTO

2.1 Misure Tecniche ed 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 tenendo conto dello stato dell'arte, dei costi di implementazione, della natura, ambito, contesto e finalità del trattamento dei Dati Personali.

L'Appendice 2 si applica solo nella misura in cui tali Servizi SAP vengano eseguiti presso o da sedi SAP. Nel caso in cui SAP stia eseguendo i Servizi SAP presso le sedi del Cliente e venga concesso a SAP l'accesso ai sistemi e ai dati del Cliente, SAP dovrà rispettare le ragionevoli condizioni amministrative, tecniche e fisiche messe del Cliente per proteggere tali dati e proteggerli da accessi non autorizzati. In relazione ad eventuali accessi ai sistemi e ai dati del Cliente, il Cliente dovrà fornire al personale SAP le autorizzazioni utente e le password per accedere ai suoi sistemi, nonchè di revocare tali autorizzazioni e far cessare tale accesso, qualora il Cliente lo ritenga di volta in volta appropriato. Il Cliente non concederà a SAP l'accesso ai sistemi o alle informazioni personali del Licenziatario (del Cliente o di terzi) a meno che tale accesso non sia essenziale per lo svolgimento dei Servizi SAP. Il Cliente non dovrà archiviare alcun Dato Personale negli ambienti non-produttivi.

2.2 Modifiche. SAP applica le misure tecnico-organizzative stabilite all'Appendice 2 all'intera base clienti SAP e che ricevono il medesimo Servizio SAP. SAP potrà modificare le misure indicate

all'Appendice 2 in qualsiasi momento e senza preavviso purchè 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 provenienti dal Cliente. SAP tratterà i Dati Personali solo in conformità alle istruzioni documentate del Cliente. Il Contratto (incluso il presente DPA) rappresenta tali istruzioni documentate e il Cliente potrà fornire ulteriori istruzioni durante l'esecuzione del Servizio SAP. SAP farà quanto ragionevolmente possibile per implementare le eventuali altre istruzioni del Cliente, sempre che siano richieste dalla Normativa sulla Protezione dei Dati, tecnicamente fattibili e non richiedano modifiche all'esecuzione del Servizio SAP. 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 dovrà informare 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 potranno concedere l'accesso solamente a persone autorizzate che si siano impegnate alla riservatezza. SAP e i Sub-responsabili formeranno regolarmente il personale che ha accesso ai Dati Personali sulle applicabili misure di sicurezza dei dati 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 o eventuali Violazioni dei Dati Personali. SAP comunicherà al Cliente, non appena sia ragionevolmente possibile, eventuali richieste ricevute da un Soggetto Interessato in relazione ai Dati Personali senza rispondere essa stessa a tale richiesta in mancanza di eventuali ulteriori istruzioni del Cliente. SAP provvederà a correggere o rimuovere eventuali Dati Personali in suo possesso (ove possibile), 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 Accertamento 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 Servizio SAP (ad esempio, il presente DPA, il Contratto, relazioni di revisione o certificazioni). L'eventuale ulteriore supporto andrà concordato dalle Parti.

4. ELIMINAZIONE DEI DATI

Il Cliente ordina a SAP di cancellare Dati Personali ancora custoditi da SAP (se presenti) entro un ragionevole periodo di tempo in linea con la Normativa sulla Protezione dei Dati (che non potrà eccedere i sei mesi), una volta che i Dati Personali non siano più necessari all'esecuzione del Contratto, a meno 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 non siano in possesso delle idonee qualificazioni o indipendenti) potranno verificare i centri di servizo e di supporto e le pratiche di sicurezza informatica di SAP relative ai Dati Personali trattati da SAP solamente se:

(a) SAP non abbia fornito suffiente evidenza della sua conformità con le misure tecniche ed organizzative fornendo una certificazione di conformità alla norma ISO 27001 o ad altri standard (nell'estensione di cui al certificato). Le certificazioni sono disponibili all'indirizzo: https://www.sap.com/corporate/en/company/quality.html#certificates o su richiesta nel caso in cui la certificazione non sia disponibile online; o

(b) Si è verificata una Violazione dei Dati personali; oppure

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

(d) La Normativa obbligatoria sulla Protezione dei Dati Personali riconosca al Cliente un diritto per la 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 garantire un preavviso minimo 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, l'intervallo temporale e l'ambito di qualsiasi verifica andrà concordata dalle parti che agiranno ragionevolmente e in buona fede. Per quanto possibile, le verifiche del Cliente dovranno limitarsi a verifiche in remoto. Nel caso siano obbligatorie verifiche in loco, non potranno estendersi per più di un giorno lavorativo. Oltre tale limitazioni, le parti utilizzeranno le certificazioni in vigore o 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 di un 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;

(c) Con riguardo al SAP Support, la lista di Sub-responsabili di SAP in vigore alla data di decorrenza del Contratto sia resa pubblica da SAP (pubblicata al seguente indirizzo: https://support.sap.com/en/my-support/subprocessors.html) 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 Servizio SAP; e

(d) Con riguardo ai Professional Services, SAP dovrà, su richiesta del Cliente, mettere a disposizione l'elenco o identificare tali Sub-responsabili prima dell'avvio dei relativi Servizi SAP.

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 l'intenzione di aggiungere o sostituire all'elenco dei Sub-responsabili ivi compreso il nominativo, l'indirizzo e la qualifica del nuovo Sub-responsabile o (i) relativamente al SAP Support - mediante pubblicazione sul SAP Support Portal o a mezzo di e-mail, a seguito della registrazione del Cliente sul SAP Portal e (ii) relativamente ai Professional Services - mediante pubblicazione analoga sul SAP Support Portal, o a mezzo di e-mail, o in altra forma scritta; 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) SAP Support: Qualora il Cliente 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 SAP Support dandone comunicazione scritta a SAP, tale comunicazione dovrà pervenire a SAP non oltre trenta giorni dalla data della comunicazione inviata da SAP al Cliente del nuovo Sub-responsabile. Nel caso in cui il Cliente non invii a SAP una comunicazione di recesso entro tale termine di trenta giorni, si riterrà che il Cliente abbia accettato il nuovo Sub-responsabile. 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 inviare a SAP una comunicazione di risoluzione e non inficieranno il diritto di SAP di utilizzare il nuovo Sub-responsabile successivamente il periodo di trenta giorni.

(b) Professional Service: Qualora il Cliente abbia una fondato motivo, ai sensi della Normativa sulla Protezione dei Dati, relativo al trattamento dei Dati Personali da parte dei Sub-responsabili, il Cliente potrà opporsi all'utilizzo del Sub-responsabile da parte di SAP, mediante comunicazione scritta a SAP entro cinque giorni lavorativi dalla comunicazione di SAP ai sensi della Clausola 6.2. Qualora il Cliente contesti l'utilizzo del Sub-responsabile, le parti si riuniranno in buona fede per discutere una soluzione. SAP potrà scegliere di: (i) non utilizzare il Sub-responsabile o (ii) adottare le misure correttive richieste dal Cliente nella sua obiezione e utilizzare il Sub-responsabile. Nel caso in cui nessuna di tali opzioni sia ragionevolmente possibile e il Cliente continui ad opposrsi per fondati motivi, ciascuna delle parti potrà recedere dai relativi servizi con preavviso scritto di cinque giorni. Nel caso in cui il Cliente non si opponga entro cinque giorni dalla ricezione della comunicazione, si riterrà che il Cliente abbia accettato il nuovo Sub-responsabile. Qualora l'obiezione del Cliente rimanga irrisolta trenta giorni dopo dalla sua presentazione, e SAP non abbia ricevuto alcuna comunicazione di recesso, il Sub-responsabile si riterrà accettato dal Cliente.

(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 relativo Sub-responsabile interessato con una delle seguenti modalità (i) il Cliente potrà benficiare delle Clausole Contrattuali Standard stipulate da SAP o SAP SE e il Sub-responsabile acquisendo i relativi diritti e obbligazioni ("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), o (d) una comunicazione al Cliente; e/o
- **(c)** Altri titolari autorizzati dal Cliente ad includere i Dati Personali ai sensi del Contratto possono altresì aderire alle Clausole Contrattuali Standard con SAP e/o 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 rischiesti dalla Normativa sul Trattamento dei Dati. Ciascuna delle parti 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. DEFINIZIONI

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

9.1 "Utenti Autorizzati" si riferisce a qualunque persona a cui il Cliente concede l'autorizzazione di accesso in conformità con una licenza software SAP per utilizzare il Servizio SAP che sia un dipendente, agente, appaltatore o rappresentante (i) del Cliente, (ii) delle Affiliate del Cliente, e/o

(iii) dei Business Partner del Cliente e delle Affiliate del Cliente (come definiti nel Contratto di Licenza Software e Supporto).

9.2 **"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.

9.3 **"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).

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

9.5 **"Dati Personali"** si riferisce a qualsiasi 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 forniti a o ai quali SAP o i suoi Sub-responsabili hanno accesso al fine di fornire il Servizio SAP ai sensi del presente Contratto.

9.6 **"Violazione dei Dati Personali"** si riferisce ad una (1) confermata 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.

9.7 **"Professional Service"** si riferisce ai servizi di implementazione, ai servizi di consulenza e/o i servizi quali i SAP Premium Engagement Support Services, Innovative Business Solutions Development Services, Innovative Business Solutions Development Support Services.

9.8 **"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.

9.9 **"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).

9.10 **"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 Servizio SAP e che trattano i Dati Personali ai sensi del presente DPA.

Appendice 1 al DPA e, alle eventuali Clausole Contrattuali Standard

Esportatore
L'Esportatore è il Cliente che ha concluso un Contratto di Licenza Software e Supporto e/o un Contratto di Servizio con SAP ai sensi del quale esso beneficia del SAP Service come descritto nel relativo Contratto. L'Esportatore dei Dati permette ai Titolari di utilizzare anche il SAP Service, tali altri Titolari sono anche Esportatori.

Importatore
SAP ed i propri Sub-responsabili forniscono il SAP Service quale definito ai sensi del relativo Contratto stipulato dall'Esportatore che comprende il seguente SAP Service:

- Ai sensi del Contratto di Licenza Software e Supporto: SAP e/o i suoi Sub-responsabili forniscono supporto allorquando un Cliente presenti un ticket di assistenza perché il Software non è disponibile o non sta funzionando come previsto. Essi rispondono alle chiamate telefoniche ed eseguono attività di ricerca guasti di base e gestisce i ticket di assistenza in un sistema di tracciatura.
- ai sensi del Services Agreement for Professional Services: SAP e/o i suoi Sub-responsabili forniscono i Servizi ai sensi del Modulo d'Ordine Servizi e del Documento d'Ambito applicabile.

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 tramessi al, messi a disposizione del o a cui l'Importatore acceda.

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

Il Cliente stabilisce le categorie di dati e/o i campi di dati che possono essere trasferiti mediante il SAP Service come indicato nel relativo Contratto. 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 trasferito da Utenti Autorizzati e può comprendere dati finanziari quali i dati riguardanti il conto corrente 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 soggetti alle attività di elaborazione di base stabilite nel Contratto che possono comprendere:

- l'utilizzo dei Dati Personali per fornire il SAP Service
- la custodia dei Dati Personali
- l'elaborazione informatica dei Dati Personali per la trasmissione dei dati
- l'esecuzione delle istruzioni del Cliente ai sensi del Contratto

Appendice 2 al DPA e alle eventuali Clausole Contrattuali Standard – Misure Tecnico-Organizzative

1. MISURE TECNICO-ORGANIZZATIVE

Le seguenti 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 migliore livello di sicurezza. Le misure individuali possono essere rimpiazzate 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 i SAP 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 una rigorosa 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 SAP Services ai sensi del relativo 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.
- All'atto del trasferimento dei dati tra SAP e i suoi clienti le misure di protezione necessarie al trasferimento dei dati vengono con il presente concordati tra SAP ed il proprio cliente e vengono resi parte integrante del 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 SAP Service nella misura tecnicamente possibile.

1.6 Controllo Job. Il Controllo Job è necessario ad assicurare che i dati personali trattati per conto di altri siano trattati in stretta osservanza delle istruzioni del 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.

  Relativamente al SAP Support, i clienti SAP hanno il controllo costante sulle proprie connessioni remote di supporto. I dipendenti SAP non possono accedere ad un sistema di un cliente senza avere informato o con consenso del cliente. Per SAP Support, SAP fornisce una facility per i ticket di supporto appositamente progettata e sicura nella quale SAP fornisce un'area di sicurezza soggetta a specifici controlli di accesso e monitoraggio per il trasferimento di dati di accesso e password. I clienti SAP hanno il controllo costante sulle proprie connessioni remote di supporto. I dipendenti SAP non possono accedere ad un sistema on premise di un cliente senza avere informato e la collaborazione attiva del cliente.

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 continuità dell'attività per i processi fondamentali.
- 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 controlli tecnici idonei per assicurare in ogni momento la separazione dei Dati Cliente.
- Il Cliente (ivi compresi i suoi Titolari approvati) avrà accesso solamente ai propri Dati sulla base di autenticazioni ed autorizzazioni sicure.
- 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 del DPA

La seguente tabella indica gli Articoli del GDPR aventi rilevanza 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	Scopi ed Applicazione. Struttura.
28(3) (a) e 29	3.1 e 3.2	Istruzioni provenienti dal 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	Eliminazione dei Dati
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.

Allegato 4
CLAUSOLE CONTRATTUALI STANDARD («INCARICATI DEL TRATTAMENTO»)[1]

Le Clausole Contrattuali Standard cui fa riferimento il presente DPA sono disponibili al seguente link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087.

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