HITACHI ENERGY TERMINI E CONDIZIONI GENERALI PER L'ACQUISTO DI SERVIZI IT CLOUD PROGRAMMA SPECIFICO (2023-1 ITALIA)

1. DEFINIZIONI AGGIUNTIVE

Oltre alle definizioni di cui alla Clausola 1 delle CG, nel presente Allegato specifico si applicano le seguenti definizioni:

Termine di accesso : indica il termine per il quale deve essere il Cliente

fornito i Servizi Cloud, come specificato nell'Ordine;

Servizi Cloud : indica quei Servizi forniti dal Fornitore che sono indicati nell'Ordine come forniti su base "Software as a Service", "Platform as a Service", "Infrastructure as a Service" o "Cloud" o dove esiste un riferimento a questo Allegato specifico nell'Ordine;

Software Cloud : indica i programmi per computer elencati nell'Ordine e qualsiasi Modifica fornita dal Fornitore durante la durata del Contratto;

Titolare : indica il soggetto che determina le finalità e i mezzi a del Trattamento dei Dati Personali;

Contenuto Cloud del Cliente : indica i dati (che possono essere Materiali del Cliente e includere Dati Personali) che sono archiviati, utilizzati e/o elaborati dai sistemi informatici del Fornitore;

Interessato: indica la persona fisica identificata o identificabile cui si riferiscono i Dati Personali;

Piano di Disaster Recovery : indica un piano che stabilisce le procedure da adottare per consentire il ripristino o la prosecuzione di un Servizio Cloud a seguito di un disastro naturale o indotto dall'uomo, comprese le procedure che il Fornitore deve adottare per pianificare e prevedere tali evento;

Documentazione : indica la documentazione fornita al Cliente dal Fornitore in relazione al Software Cloud, inclusa la Specifica e qualsiasi manuale utente o altra documentazione fornita ai sensi del Contratto, e inclusa la documentazione descritta nell'Ordine;

SEE : indica lo Spazio economico europeo: gli Stati membri dell'Unione europea insieme a Islanda, Liechtenstein e Norvegia; UE : indica l'Unione Europea;

Rilascio di manutenzione : indica una versione del Software Cloud che corregge i guasti, aggiunge funzionalità o in altro modo modifica o aggiorna il Software Cloud;

Modifica : indica qualsiasi Rilascio di Manutenzione o modifica specifica del Cliente;

Trattamento : indica qualsiasi operazione o insieme di operazioni eseguite sui Dati Personali, anche con mezzi automatici, come raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, reperimento, consultazione, utilizzo, divulgazione mediante trasmissione, diffusione o altrimenti messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione;

Responsabile del trattamento: indica il soggetto che tratta i Dati Personali per conto del Titolare;

Security Audit : ha il significato di cui alla Clausola 7.3;

Specifica : indica la specificazione dei Servizi Cloud forniti nell'ambito del Contratto come definiti nell'Ordine;

2. APPLICAZIONE DI QUESTO SPECIFICO SCHEDA

Il presente Programma specifico si applica a tutti i Servizi Cloud forniti dal Fornitore, come stabilito nell'Ordine.

3. IMPLEMENTAZIONE

3.1 Il Fornitore deve svolgere tutte le attività ad esso assegnate nell'Ordine ed eseguire tutte le altre attività (diverse da quelle assegnate al Cliente nell'Ordine) necessarie per implementare i Servizi Cloud (i "Servizi di Implementazione").

3.2 Salvo quanto diversamente concordato nell'Ordine, i Servizi di implementazione sono soggetti all'accettazione del Cliente. Il Fornitore dovrà fornire i Servizi di implementazione in modo tempestivo e così via in modo da garantire il rispetto di qualsiasi traguardo o data di scadenza specificata nell'Ordine.

3.3 Il Fornitore dovrà fornire al Cliente relazioni periodiche sullo stato di avanzamento che (con ragionevole dettaglio) descrivono lo stato attuale dei Servizi di implementazione e identificano eventuali problemi o ritardi effettivi o previsti (insieme ai dettagli di tutte le azioni intraprese o da intraprendere per porre rimedio a tali problemi o ritardi).

4. SERVIZI CLOUD

4.1 Il Fornitore dovrà fornire i Servizi Cloud in conformità al Contratto. Il Fornitore deve fornire i Servizi Cloud da strutture e utilizzando l'architettura e il personale IT con sede nel Regno Unito, nell'UE, nel SEE o in Svizzera, salvo diverso accordo scritto del Cliente.

4.2 Il Fornitore concede a ciascun membro del Gruppo Clienti, durante il Periodo di Accesso, una licenza mondiale, esente da royalty e non esclusiva per:

4.2.1 utilizzare i Servizi Cloud;

4.2.2 accedere e utilizzare il Software Cloud tramite i Servizi Cloud; e

4.2.3 utilizzare il Software Cloud (e la Documentazione) in relazione a qualsiasi attività commerciale del Gruppo Clienti.

4.3 Il Cliente può concedere una sub-licenza dei propri diritti ai sensi della Clausola 4.2 a qualsiasi Fornitore di terze parti allo scopo che tale Fornitore di terze parti fornisca beni, software e/o servizi al Gruppo di Clienti.

4.4 Il Cliente riconosce di non avere alcun diritto, titolo o interesse nel Software Cloud o nella Documentazione salvo quanto stabilito nel Contratto.

4.5 Salvo quanto consentito dal Contratto, il Cliente non deve:

4.5.1 distribuire, concedere in sublicenza o altrimenti trasferire tutto o parte del Software Cloud a qualsiasi altra persona;

4.5.2 laddove nell'Ordine sia specificato un numero massimo di utenti del Servizio Cloud, consentire l'accesso e l'utilizzo del Servizio Cloud in numero superiore al numero massimo di utenti autorizzati;

4.5.3 utilizzare il Software Cloud come service bureau o in qualsiasi attività simile a beneficio di qualsiasi persona che non sia un membro del Gruppo Clienti;

4.5.4 decodificare, decompilare o disassemblare il Software Cloud salvo quanto consentito dalle leggi applicabili;

4.5.5 rimuovere, cancellare o alterare qualsiasi diritto d'autore, avviso di proprietà o simile sul Software Cloud; o

4.5.6 accedere, archiviare, distribuire o trasmettere intenzionalmente virus o altri software dannosi o qualsiasi materiale durante l'utilizzo dei Servizi Cloud che:

a) è illegale, dannoso, minaccioso, diffamatorio, osceno, offensivo, molesto o offensivo dal punto di vista razziale o etnico;
b) facilita l'attività illegale;
c) raffigura immagini sessualmente esplicite;
d) promuove la violenza illegale;
e) è discriminatorio in base a razza, sesso, colore, credo religioso, orientamento sessuale, disabilità; o
f) in un modo che sia altrimenti illegale o causi danni o lesioni a persone o cose.

5. CONTENUTI CLIENTI

5.1 In deroga alla Clausola 10.5 delle CG:

5.1.1 I Contenuti Customer Cloud saranno e rimarranno di proprietà del Cliente;

5.1.2 Il Fornitore e il Team del Fornitore non avranno il diritto di utilizzare o accedere ad alcun Contenuto Cloud del Cliente; e

5.1.3 Il Fornitore non deve utilizzare, archiviare, copiare o divulgare alcun Contenuto Cloud del Cliente salvo quanto necessario per l'adempimento dei propri obblighi ai sensi del Contratto o come altrimenti espressamente autorizzato per iscritto dal Cliente.

5.2 Il Fornitore deve assicurarsi che il Team del Fornitore (o qualsiasi altro dipendente, agente o subappaltatore del Fornitore) non tenti di accedere o consentire l'accesso a qualsiasi Contenuto Cloud del Cliente a cui non ha diritto.

5.3 Immediatamente su richiesta del Cliente e alla scadenza del contratto, il Fornitore sovrascriverà o cancellerà in modo permanente dai propri sistemi informatici tutte le copie dei Contenuti Cloud del Cliente (ad eccezione delle copie dei Contenuti Cloud del Cliente archiviate su backup dei sistemi del Fornitore che non possono essere cancellati con sforzi ragionevoli).

5.4 Il Cliente dovrà indennizzare e tenere indenne il Fornitore da e contro tutti i costi, reclami, richieste, responsabilità, spese, danni o perdite (incluse eventuali perdite consequenziali dirette o indirette, mancato profitto e tutti gli interessi, sanzioni e costi e spese legali e professionali) derivanti da un'affermazione secondo cui la fornitura dei Contenuti Cloud del Cliente al Fornitore viola i Diritti di proprietà intellettuale di terzi.

6. GARANZIE NUVOLA

6.1 In aggiunta a qualsiasi garanzia fornita dal Fornitore nelle CGC, il Fornitore dichiara, garantisce e si impegna che il Software Cloud nel suo insieme e ogni singola Modifica:

6.1.1 durante la durata del Contratto, essere esenti da vizi materiali; e

6.1.2 rispettare ed eseguire in conformità con la Documentazione.

6.2 Senza limitare la Clausola 6.1, il Fornitore dichiara, garantisce e si impegna che ciascuna Modifica non degraderà la funzionalità o le prestazioni del Software Cloud.

6.3 Il Fornitore dichiara, garantisce e si impegna che, quando consegnato al Cliente o altrimenti implementato dal Fornitore ai sensi del Contratto:

6.3.1 non inserirà né includerà, né consentirà o farà in modo che alcuna persona o software inserisca o includa alcun Software dannoso nel Software Cloud nel suo insieme o in qualsiasi singola Modifica;

6.3.2 utilizzerà un software antivirus aggiornato e accettato dal settore per verificare e prevenire l'introduzione di software dannoso o virus nel Software Cloud nel suo insieme o in qualsiasi singola Modifica; e

6.3.3 coopererà con il Cliente per mitigare l'effetto di qualsiasi software dannoso o virus trovato nel Software Cloud nel suo insieme o in qualsiasi singola Modifica.

6.4 Il Fornitore dichiara e garantisce di aver ottenuto, e si impegna a mantenere durante il Periodo di Accesso, tutti i consensi, le licenze e le autorizzazioni da esso richieste per adempiere ai propri obblighi ai sensi del Contratto.

6.5 Il Fornitore dichiara, garantisce e si impegna che, salvo quanto diversamente concordato nell'Ordine, i Servizi Cloud rispetteranno gli standard, i controlli e i requisiti di sicurezza stabiliti nella norma ISO 27001:2013, SOC 1 tipo II e/o SOC 2 tipo II compreso il suo utilizzo -principi di fiducia delle capacità.

6.6 Si applicano i rimedi di cui alla Clausola 6.2 delle CG.

7. SICUREZZA CLOUD E OBBLIGHI DI AUDIT

7.1 Il fornitore, a proprie spese, farà in modo che un fornitore autorizzato di servizi di attestazione e conformità fornisca al Cliente e ai suoi revisori una volta all'anno un rapporto di audit ISO 27001:2013, SOC 1 tipo II e SOC 2 tipo II sui controlli effettuati e sui test dell'efficacia operativa presso le strutture del Fornitore e dei fornitori di servizi del Fornitore in relazione ai Servizi Cloud.

7.2 Eventuali certificazioni e rapporti di audit di cui alla Clausola 7.1 e qualsiasi altra informazione richiesta dal Cliente. Il Fornitore si prepara come standard per gli altri suoi clienti, sarà fornito senza costi aggiuntivi per il Cliente.

7.3 Salvo quanto diversamente previsto nell'Ordine, su richiesta del Cliente (non più di una volta per anno solare e in aggiunta in caso di incidente di sicurezza, mancato rispetto da parte del Fornitore dei propri obblighi di sicurezza e/o requisiti normativi) il Cliente può condurre un audit di sicurezza per verificare il rispetto da parte del Fornitore degli obblighi di sicurezza previsti dal Contratto ("Security Audit"). Tale Audit di sicurezza può essere condotto dal Cliente o da un revisore di terze parti, a condizione che il Cliente e/o revisori di terze parti accettino termini di riservatezza ragionevolmente accettabili. Salvo in caso di requisiti normativi o altre circostanze che richiedono un'azione tempestiva, il Cliente dovrà fornire un preavviso scritto di almeno trenta (30) giorni della propria intenzione di condurre un audit di sicurezza. Il Cliente dovrà condurre l'audit in modo rapido, entro un tempo ragionevole e in modo da non interrompere irragionevolmente le operazioni quotidiane del Fornitore. Il Fornitore dovrà cooperare ragionevolmente e fornire tale documentazione e l'accesso come ragionevolmente richiesto dal Cliente per condurre un audit di sicurezza. A scanso di equivoci, il Fornitore non sarà in alcun caso obbligato a fornire informazioni relative ad altri clienti.

7.4 Il Fornitore dovrà rispettare gli eventuali requisiti aggiuntivi di sicurezza, audit e rendicontazione specificati nell'Ordine.

7.5 Il Fornitore dovrà applicare il Piano di Disaster Recovery come indicato nell'Allegato 1 al presente Allegato specifico.

8. PROTEZIONE DATI

8.1 Nel fornire i Servizi Cloud, il Fornitore tratta i Dati Personali in qualità di Responsabile del trattamento secondo le istruzioni del Cliente che agisce in qualità di Titolare, in conformità con l'Allegato sul Trattamento dei Dati di cui all'Allegato 2 al presente Allegato specifico.

ALLEGATO 1

PIANO DI RIPRESA DA DISASTRO

ALLEGATO 2

ALLEGATO TRATTAMENTO DEI DATI ("DPA")

1. ISTRUZIONI DEL CLIENTE AL FORNITORE

1.1 Il Fornitore seguirà le istruzioni ricevute dal Cliente in merito al Trattamento dei Dati Personali.

1.2 Il Cliente istruisce il Fornitore a raccogliere, elaborare e utilizzare i Dati Personali per fornire i servizi come concordato nell'Ordine. Ulteriori istruzioni possono essere impartite dal Cliente.

1.3 Il Fornitore informerà immediatamente il Cliente se considera eventuali istruzioni per violare le leggi sulla protezione dei dati applicabili.

2. OBBLIGHI DEL FORNITORE

2.1 Il Fornitore non utilizzerà i Dati Personali per scopi diversi da quelli descritti nell'Ordine.

2.2 Obblighi nei confronti del Personale del Fornitore

2.2.1 Riservatezza. Il Fornitore dovrà garantire che il proprio personale coinvolto nel Trattamento dei Dati Personali ai sensi del presente DPA sia vincolato alla riservatezza e gli sia vietato accedere, elaborare e/o utilizzare i Dati Personali senza autorizzazione e per finalità diverse dall'adempimento degli obblighi contrattuali del Fornitore nei confronti -vis cliente.

2.2.2 Su richiesta del Cliente, il Fornitore fornirà al Cliente il proprio modulo standard sulla segretezza dei dati personali e gli accordi di riservatezza o il linguaggio del modello e, se richiesto ai sensi di un audit o della legge applicabile, la prova che il personale pertinente è effettivamente obbligato da tali accordi di segretezza e riservatezza dei dati, che sopravvivono al cessazione dell'assunzione del personale.

2.2.3 Affidabilità. Il Fornitore dovrà garantire l'affidabilità di tutto il personale coinvolto nel Trattamento dei Dati Personali.

2.2.4 Il Fornitore familiarizzerà tutte le persone che hanno accesso ai Dati Personali del Cliente con le disposizioni sulla protezione dei dati rilevanti per il loro lavoro.

2.2.5 Limitazione dell'accesso: Il Fornitore dovrà garantire che l'accesso del personale del Fornitore ai Dati Personali sia limitato al personale che esegue servizi in conformità con l'Ordine.

2.3 Assistenza del Fornitore al Cliente

Il Fornitore assisterà ragionevolmente il Cliente nell'adempimento dei propri obblighi ai sensi del GDPR e nella gestione delle richieste e dei reclami dell'Interessato. Ciò vale in particolare per quanto riguarda:

2.3.1 Obbligo del Cliente di adempiere ai propri obblighi (rispetto alle Valutazioni di Impatto sulla Protezione dei Dati e alla Consultazione preventiva con un'autorità di controllo) ai sensi degli articoli da 35 a 36 GDPR;

2.3.2 qualsiasi richiesta avanzata da un'autorità di controllo nei confronti del Cliente in relazione al Trattamento dei Dati Personali nell'ambito dell'Ordine; e

2.3.3 qualsiasi reclamo o ispezione o procedura a cui il Cliente è soggetto e che si riferisce al trattamento dei Dati Personali da parte del Fornitore.

2.4 Il Fornitore informerà immediatamente il Cliente di eventuali ispezioni, indagini e/o misure condotte e/o di qualsiasi procedimento penale, amministrativo o sommario illecito da parte di un'autorità competente e relativo a Dati Personali o relativo al trattamento di Dati Personali in relazione all'Ordine.

2.5 Il Fornitore informerà immediatamente il Cliente di qualsiasi richiesta di divulgazione di Dati personali da parte di un'autorità di contrasto, di un'agenzia di intelligence o di altro tipo di richiesta di accesso del governo, a meno che tale notifica non sia vietata dalla legge applicabile. Per quanto riguarda l'eventuale accesso da parte delle autorità pubbliche ai Dati Personali trasferiti in un "paese terzo" ai sensi della sezione 6.3, disciplinata dalle Clausole contrattuali standard dell'UE di cui all'Allegato 4, si applicherà l'"Appendice sulle misure supplementari" dell'Allegato 4.A.Il Fornitore informerà il Cliente del punto di contatto del Fornitore per tutte le questioni relative alla privacy e alla protezione dei dati nell'ambito dell'Ordine.

2.6 Il Fornitore dovrà monitorare i processi interni e aggiornare le misure tecniche e organizzative per garantire che il trattamento nell'ambito della sua area di responsabilità sia conforme alle leggi sulla protezione dei dati applicabili.

3. SUB-PROCESSORI

3.1 Il Cliente acconsente che il Fornitore possa assumere i sub-responsabili identificati nell'Allegato 3.

3.2 Eventuali sub-incaricati a cui il Fornitore trasferisce Dati Personali, anche quelli utilizzati a fini di conservazione, avranno stipulato accordi scritti con il Fornitore non meno protettivi del presente DPA.

3.3 Salvo quanto stabilito nel DPA, o come diversamente autorizzato dal Cliente per iscritto, il Fornitore non trasferirà a terzi (nemmeno per finalità di archiviazione o supporto remoto) i Dati Personali forniti dal Cliente al Fornitore per le finalità descritte nel Contratto.

3.4 Il Fornitore è responsabile per gli atti e le omissioni dei suoi sub-incaricati nella stessa misura in cui il Fornitore sarebbe responsabile se prestasse i servizi di ciascun sub-incaricato direttamente ai termini del presente DPA, salvo quanto diversamente stabilito nell'Ordine.

4. DIRITTI DEGLI INTERESSATI

4.1 Il Fornitore non può, di propria iniziativa, correggere, rettificare, rimuovere, limitare, bloccare o esportare Dati Personali.

4.2 Il Fornitore può consentire al Cliente di correggere, rettificare, rimuovere, limitare, bloccare o esportare i propri Dati Personali, oppure correggere, rettificare, rimuovere, limitare, bloccare o esportare qualsiasi Dati Personali senza indebito ritardo, comunque non oltre dieci

(10) giorni su istruzioni del Cliente.

4.3 Se un Interessato contatta direttamente il Fornitore per qualsiasi richiesta o richiesta, il Fornitore informerà il Cliente della richiesta o richiesta senza indebito ritardo. Il Fornitore supporterà ragionevolmente i Clienti nell'affrontare tali richieste o richieste.

5. VIOLAZIONE DELLA SICUREZZA E NOTIFICA

5.1 Il Fornitore dovrà informare il Cliente senza indebito ritardo dopo essere venuto a conoscenza di qualsiasi violazione della sicurezza presso il Fornitore che porti alla distruzione, perdita, alterazione, divulgazione non autorizzata o accesso non autorizzato ai Dati Personali, trasmessi, archiviati o altrimenti elaborati dal Fornitore o dal suo sub -processori.

5.2 La notifica deve contenere almeno:

- una descrizione della natura della violazione della sicurezza compresi, ove possibile, le categorie e il numero approssimativo di Interessati interessati dalla violazione e le categorie e il numero approssimativo di record di Dati personali interessati;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto da cui è possibile ottenere ulteriori informazioni;
- una descrizione delle probabili conseguenze della violazione della sicurezza;
- una descrizione delle misure adottate o proposte dal Fornitore per porre rimedio alla violazione della sicurezza, comprese, se del caso, misure per mitigare eventuali conseguenze negative.

Se, e nella misura in cui non è possibile fornire tutte queste informazioni contemporaneamente, le informazioni possono essere comunicate in modo scaglionato senza indebito ritardo.

5.3 Il Cliente istruisce il Fornitore ad adottare tutte le misure che il Fornitore ritiene necessarie o utili per proteggere i Dati Personali trattati per conto del Cliente e per ridurre al minimo le possibili conseguenze negative per gli Interessati.

6. LUOGO DI LAVORAZIONE E TRASFERIMENTI INTERNAZIONALI

6.1 Il Fornitore tratterà i Dati Personali esclusivamente all'interno di uno Stato membro dell'UE, del SEE o della Svizzera. Ogni trattamento (compresa la mera possibilità di accesso) al di fuori di questi territori richiede il previo consenso scritto del Cliente.

6.2 Oltre al requisito dell'approvazione del Cliente di cui al punto 6.1, ogni trasferimento di dati verso uno Stato che non sia uno Stato membro dell'UE, del SEE o della Svizzera avverrà solo se le condizioni specifiche degli articoli 44 e segg. GDPR sono stati rispettati. I Dati Personali possono essere trasferiti solo verso Paesi terzi, per i quali non è stata presa una decisione di adeguatezza ai sensi dell'articolo 45 GDPR, se tale trasferimento può essere legittimato concordando le Clausole Contrattuali Standard dell'UE. Su richiesta del Cliente, il Fornitore fornirà detta documentazione al Cliente.

6.3 Se e nella misura in cui i Dati Personali vengono trasferiti a un paese terzo, le Parti concordano che le clausole contrattuali standard dell'UE qui allegate come Allegato 4 si applicheranno a qualsiasi trasferimento di questo tipo tra Cliente e Fornitore, nonché l'"Appendice sulle misure supplementari" in Allegato 4.A. A scanso di equivoci, ciò vale anche per i trasferimenti di Dati Personali nel Regno Unito se la Commissione Europea non ha fornito lo stato di adeguatezza al Regno Unito al termine del periodo di transizione Brexit.

6.4 Su richiesta del Cliente, il Fornitore dovrà stipulare qualsiasi accordo aggiuntivo sul trattamento dei dati o accordo aggiuntivo sulla protezione dei dati come richiesto dalla legge obbligatoria sulla protezione dei dati o da un'autorità competente per la protezione dei dati o da un'altra autorità competente, o in qualsiasi versione aggiornata delle clausole contrattuali standard dell'UE con il Cliente. Il Fornitore dovrà garantire che i suoi Affiliati o sub-incaricati pertinenti, su richiesta del Cliente, stipulino tempestivamente qualsiasi accordo di questo tipo con il Cliente.

7. MISURE TECNICHE E ORGANIZZATIVE

7.1 Il Fornitore attuerà e manterrà misure tecniche e organizzative adeguate per la protezione della sicurezza (compresa la protezione contro il Trattamento non autorizzato o illecito e contro la distruzione, la perdita o l'alterazione accidentale o illegale, la divulgazione o l'accesso non autorizzati ai Dati Personali), la riservatezza e integrità dei Dati Personali, come indicato nell'Allegato 2 al presente DPA.

7.2 Se il Fornitore, o qualsiasi sub-incaricato, rientra nella Sezione 702 degli Stati Uniti FISA, il Fornitore attuerà misure tecniche per rendere impossibile o inefficace l'accesso ai Dati Personali. Lo stesso vale se il Fornitore, o qualsiasi sub-responsabile del trattamento, tratta dati in un "paese terzo" in cui le autorità pubbliche possono richiedere l'accesso ai Dati personali, laddove tale accesso vada oltre quanto necessario e proporzionato in una società democratica.

7.3 Su richiesta del Cliente, il Fornitore fornirà evidenza dell'efficacia delle misure tecniche e organizzative attraverso

7.4 (i) certificati, rapporti o estratti di rapporti forniti da organismi indipendenti (es. revisore dei conti, responsabile della protezione dei dati, dipartimento di sicurezza informatica, revisore della privacy dei dati, revisore della qualità) o (ii) un'adeguata certificazione della sicurezza informatica o dei dati audit di protezione (es. ISO/IEC 27001).

7.5 Le misure tecniche e organizzative sono soggette al progresso tecnico e all'ulteriore sviluppo. Il Fornitore può modificare le misure tecniche e organizzative, a condizione che le nuove misure non siano inferiori al livello di sicurezza fornito dalle misure specificate e non causino alcuna interruzione o guasto dell'infrastruttura IT del Cliente.

7.6 Il Fornitore non ridurrà materialmente la sicurezza complessiva del Servizio Cloud durante la durata dell'Ordine. Qualora il Fornitore apporti una modifica sostanziale alle misure tecniche e organizzative, ne informerà il Cliente in tempo utile. Il Cliente ha il diritto di opporsi se ritiene che la modifica non sia all'altezza del livello di protezione dei dati, non sia in linea con la legge applicabile in materia di protezione dei dati o provochi un effetto negativo sul Cliente. Se il Cliente si oppone, il Fornitore continuerà a mantenere le misure come specificato nell'Allegato 2.

8. RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

8.1 Al termine dell'Ordine, il Fornitore dovrà, in conformità con le istruzioni del Cliente, restituire immediatamente o eliminare in modo sicuro o sovrascrivere e distruggere in modo conforme alla protezione dei dati tutti i documenti, i risultati dell'elaborazione e dell'utilizzo e i set di dati relativi all'Ordine. Ciò si applica di conseguenza a tutti i dati e/o materiali di prova, rifiuti, ridondanti e scartati. Il registro della distruzione o cancellazione deve essere fornito su richiesta.

8.2 La documentazione necessaria per dimostrare l'ordinato trattamento dei Dati Personali in conformità con il presente DPA sarà conservata dal Fornitore oltre la risoluzione dell'Ordine per la durata del rispettivo periodo di conservazione. Su richiesta del Cliente, il Fornitore fornirà detta documentazione al Cliente.

9. VARIE

In caso di contraddizione, le disposizioni del presente DPA prevalgono su quelle dell'Ordine.

ALLEGATO 1

CATEGORIE DI DATI PERSONALI, CATEGORIE DI INTERESSATI E FINALITÀ DELLA RACCOLTA, TRATTAMENTO E UTILIZZO DEI DATI PERSONALISUPPLIER'S RESPONSIBILITIES

Il presente Allegato fa parte del Garante e deve essere compilato dalle parti.

Controllore

Il titolare del trattamento è [SPECIFICARE BREVEMENTE L'ATTIVITÀ DI PG RELATIVO AL TRASFERIMENTO]

Processore

Il processore is [PER FAVORE SPECIFICARE IN BREVE IL ATTIVITA' DEL RESPONSABILE RELATIVE AL TRASFERIMENTO]

Interessati

I dati personali riguardano le seguenti categorie di interessati
[SPECIFICARE PREGO]

Esempi sono:
Dipendenti inclusi volontari, lavoratori temporanei, occasionali e di agenzia
Candidati per un impiego presso PG, Ex dipendenti, Familiari di dipendenti
Agenti, consulenti, liberi professionisti del Cliente
Prospect, clienti, partner commerciali, fornitori, partner, fornitori
Utenti del Cliente autorizzati dal Cliente a utilizzare i Servizi

Categorie di dati

I dati personali riguardano le seguenti categorie di dati [SPECIFICARE]

Esempi sono :
Nome, nome/cognome
indirizzo privato/aziendale
privato/azienda Indirizzo e-mail
Data di nascita
Sesso
di età
Elenco dei dipendenti e degli indirizzi del
cliente Registri del lavoro o delle
realizzazioni Newsletter mailing list
con indirizzi e-mail Estratti conto individuali
Bollette telefoniche dettagliate
Identificatori online (ad es. indirizzi IP,
cookie) Identificatore del dispositivo (ad es.
ID dispositivo mobile) Numero di passaporto
Informazioni sul visto
di viaggio Numero di
patente di guida
Numero di carta di
credito Documenti di formazione
Dati familiari: nome della moglie,
figli Curriculum /CV
Posizione
lavorativa / Titolo
Schede presenze
Informazioni sul
libro paga

Categorie speciali di dati (se del caso)

I dati personali riguardano le seguenti categorie particolari di dati
[SPECIFICARE PREGO]

Esempi sono:
Opinione politica
Credenza religiosa o filosofica
Razza o origine etnica
Adesione sindacale Dati
sanitari
Vita sessuale e orientamento
sessuale Dati genetici o
biometrici Immagini del viso e
impronte digitali Caselle
penali

Operazioni di elaborazione

I dati personali saranno oggetto delle seguenti attività di trattamento di base
[SPECIFICARE PREGO]

[CANCELLA ESEMPI NON APPLICABILI]

ALLEGATO 2
MISURE TECNICHE E ORGANIZZATIVE

Nell'ambito dei Servizi, il Fornitore accetta di adottare tutte le misure e le precauzioni di sicurezza necessarie in conformità con gli standard del settore riconosciuti a livello mondiale e in conformità con l'art. 5/1 f e l'art. 32 GDPR per ridurre al minimo il rischio di perdita di riservatezza, integrità e disponibilità delle Informazioni del Cliente e dei Dati Personali trattati dal Fornitore (responsabile del trattamento) per eseguire i Servizi.

Il Fornitore dovrà progettare, implementare e mantenere (incluso un processo per testare, valutare e valutare regolarmente l'efficacia) Misure tecniche e operative che proteggano la sicurezza delle Informazioni del Cliente e dei Dati Personali mentre è in possesso, custodia o controllo del Fornitore, che coprano almeno le aree seguenti :

1. POLITICHE DI SICUREZZA DELLE INFORMAZIONI

1. Il Fornitore svilupperà e manterrà politiche di sicurezza delle informazioni appropriate, allineate ai migliori standard di settore e al GDPR, che proteggano i sistemi informativi del Fornitore da perdita, danno, divulgazione non autorizzata e tutte le altre violazioni dei dati o interruzione dell'attività, comprese le informazioni sui clienti e i dati personali, ottenuti dal Fornitore per fornire i Servizi.

2. ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

1. Il Fornitore dovrà mantenere personale adeguatamente qualificato, con ruoli e responsabilità chiaramente definiti, all'interno della propria organizzazione per la sicurezza delle informazioni, per coordinare l'implementazione della sicurezza per l'organizzazione del Fornitore.
2. Il fornitore deve garantire che la gestione della sicurezza sia incorporata nella gestione del progetto.
3. Il Fornitore dovrà separare in modo efficace compiti, ruoli e responsabilità, per prevenire l'uso improprio o modifiche non autorizzate/non intenzionali delle Informazioni e dei Dati Personali del Cliente.

3. SICUREZZA DELLE RISORSE UMANE

1. Il fornitore deve assicurare che tutti i dipendenti e i subappaltatori siano sottoposti a screening dei precedenti.
2. Il Fornitore deve mantenere politiche e procedure che garantiscano l'idoneità del personale del Fornitore e dei subappaltatori in relazione ai loro ruoli e responsabilità.
3. Il Fornitore dovrà fornire un adeguato programma di sensibilizzazione e formazione sulla sicurezza delle informazioni, in modo che i dipendenti e i subappaltatori del Fornitore comprendano le proprie responsabilità in materia di sicurezza, in relazione alle Informazioni sui clienti e ai Dati personali.
4. Il Fornitore dovrà sviluppare e comunicare azioni disciplinari rivolte ai dipendenti che hanno violato le politiche e gli standard di sicurezza.
5. Il Fornitore dovrà garantire che tutte le procedure necessarie siano definite ed eseguite per i dipendenti del Fornitore in caso di cambio di ruolo, fine incarico, cessazione del rapporto di lavoro, contratto o accordo. In particolare, tutti i privilegi devono essere revocati tempestivamente.

4. GESTIONE DELLE RISORSE

1. Il fornitore deve sviluppare e implementare regole di classificazione, etichettatura e gestione delle informazioni.
2. Il Fornitore dovrà mantenere procedure per identificare, controllare e mantenere la proprietà e la classificazione di sicurezza delle principali risorse del Fornitore e delle Informazioni del Cliente e dei Dati Personali elaborati dal Fornitore.
3. Il Fornitore deve mantenere le politiche che definiscono l'uso accettabile delle informazioni e delle risorse e comunicarle a tutti gli utenti appropriati delle risorse e delle informazioni del Fornitore.

5. CONTROLLO DI ACCESSO

1. Il Fornitore dovrà implementare procedure progettate per controllare l'accesso ai sistemi informativi che elaborano le Informazioni del Cliente e i Dati Personali, compreso il fornire l'identificazione univoca dell'utente e i controlli di accesso.
2. Il Fornitore limiterà l'accesso alle Informazioni e ai Dati Personali del Cliente agli utenti autorizzati con giustificazione commerciale e seguendo la regola dei privilegi minimi.
3. Il Fornitore dovrà implementare l'autenticazione a più fattori per controllare l'accesso remoto ai sistemi informativi che elaborano le Informazioni del Cliente e i Dati Personali.
4. Il Fornitore riesamina l'elenco dei privilegi nei propri sistemi (utilizzati per fornire servizi) rispetto all'elenco dei diritti su base periodica.
5. Il Fornitore dovrà garantire l'impossibilità di accesso permanente all'ambiente di produzione per i dipendenti, che elaborano i dati in caso di risoluzione dei problemi. L'accesso dovrebbe essere consentito solo in caso di risoluzione dei problemi dopo l'approvazione e l'autenticazione della direzione.

6. CONTROLLI CRITTOGRAFICI

1. Il Fornitore dovrà sviluppare e attuare una politica sull'uso dei controlli crittografici per la protezione duratura, la riservatezza e la conservazione dell'integrità delle informazioni e dei beni sensibili. Come minimo, il Fornitore dovrà garantire che le Informazioni e i Dati Personali del Cliente siano protetti mediante crittografia al trasferimento, firma digitale e crittografia a riposo.
2. Il Fornitore svilupperà e implementerà una politica sull'uso, la protezione e la durata delle chiavi crittografiche per garantirne la protezione contro l'accesso o la modifica non autorizzati e la perdita.

7. SICUREZZA FISICA E AMBIENTALE

3. Devono essere definiti perimetri di sicurezza fisica per garantire solo l'accesso autorizzato alle strutture informatiche dell'organizzazione e devono essere implementati controlli e salvaguardie fisici e ambientali efficaci per proteggere le aree in cui le informazioni sono archiviate o elaborate.
4. Il Fornitore dovrà fornire la protezione fisica di qualsiasi attrezzatura utilizzata per l'elaborazione delle Informazioni del Cliente e dei Dati Personali, nonché di tutte le infrastrutture di supporto dei sistemi informativi.
5. Il Fornitore svilupperà, comunicherà e farà rispettare le procedure per lavorare nelle aree in cui vengono elaborati i Dati del Cliente e i Dati Personali.
6. Il Fornitore dovrà implementare una politica chiara per i supporti di memorizzazione e una politica per lo schermo trasparente per le aree in cui vengono elaborati i Dati del cliente e i Dati personali.

8. SICUREZZA DELLE OPERAZIONI

1. Il Fornitore deve mantenere un insieme adeguato di processi e procedure per la gestione efficace dei

sistemi informativi che elaborano le Informazioni del Cliente e i Dati Personali, tra cui:

- Cambio gestione
- Gestione della capacità di sistemi e componenti business-critical
- Pianificazione e accettazione del sistema
- Protezione contro i malware
- Backup regolare di informazioni e software, nonché test delle capacità di ripristino rispetto agli obiettivi relativi ai tempi di ripristino e agli obiettivi dei punti di ripristino
- Registrazione e revisione di eventi, che potrebbero avere un impatto sulla sicurezza dei sistemi informativi Disattivazione dei sistemi informativi
- Sviluppo sicuro e protezione degli ambienti di pre-produzione
- Procedure per la gestione, la manipolazione, lo smaltimento e lo stoccaggio dei supporti

2. Il Fornitore dovrà fornire e utilizzare ambienti separati per scopi di sviluppo, test e operativi.
3. Il fornitore deve garantire che i dati di produzione (dati reali) non vengano utilizzati al di fuori dell'ambiente di produzione. Se i dati di produzione devono essere copiati negli ambienti di prova, devono essere applicate tecniche di anonimizzazione/ pseudonimizzazione dei dati sicuri, per garantire che la potenziale perdita di tali dati non comporti alcun rischio per PG e i suoi obblighi contrattuali e normativi.
4. Il Fornitore dovrà definire e attuare regole sull'installazione di software da parte di dipendenti e appaltatori sui dispositivi dell'Utente finale di proprietà dell'organizzazione (stazioni di lavoro, cellulari, ecc.).
5. Il fornitore deve seguire il principio della minimizzazione dei dati, in particolare la pseudonimizzazione/l'anonimizzazione dovrebbe essere applicata durante la raccolta dei dati a fini statistici.

9. SICUREZZA DELLE COMUNICAZIONI

1. Il Fornitore dovrà gestire la sicurezza della rete per proteggere i sistemi informativi.
2. Il Fornitore applicherà misure di sicurezza proteggendo le reti utilizzate e i confini con altre reti, con mezzi che includono la segregazione della rete, l'accesso remoto sicuro, il rilevamento delle intrusioni e la protezione perimetrale.
3. Il Fornitore dovrà definire i requisiti e attuare la politica per la firma di accordi di riservatezza con parti esterne, in cui vengono scambiate informazioni non pubbliche.
4. Il Fornitore dovrà imporre lo scambio di informazioni con soggetti esterni solo attraverso modalità concordate. Per lo scambio elettronico si applicano le migliori pratiche in termini di selezione di protocolli e algoritmi crittografici.

10. ACQUISIZIONE, SVILUPPO E MANUTENZIONE SISTEMI INFORMATIVI

1. Specifica, acquisizione, sviluppo e manutenzione dei Sistemi Informativi, inclusi sia quelli acquistati da fornitori esterni che quelli prodotti internamente, il Fornitore determinerà i necessari requisiti di riservatezza, integrità e disponibilità e continuerà a riesaminarli rispetto a un profilo di rischio duraturo durante il ciclo di vita dell'utilizzo.
2. Il Fornitore dovrà definire e mantenere i principi per gli aspetti di sicurezza appropriati di qualsiasi ciclo di vita di sviluppo del software.
3. Il Fornitore identificherà e valuterà le vulnerabilità e le minacce tecniche e implementerà un'efficace politica di gestione delle patch e delle vulnerabilità progettata per rimediare ai Sistemi Informativi del Fornitore.
4. Il Fornitore assicurerà che i Sistemi che elaborano le Informazioni del Cliente ei Dati Personali siano logicamente o fisicamente separati dai dati degli altri clienti.

11. RAPPORTI CON I FORNITORI

1. Il Fornitore dovrà stabilire e mantenere accordi formali con le terze parti coinvolte nella gestione dell'erogazione del servizio dei sistemi informativi del Fornitore che elaborano le Informazioni del Cliente ei Dati Personali, incorporando ove appropriato i necessari controlli di sicurezza, le politiche e gli accordi sul livello di servizio.
2. Nessuna informazione del cliente e dati personali possono essere condivisi con terze parti (inclusi i subappaltatori) senza il consenso chiaro e inequivocabile del cliente.

12. GESTIONE DEGLI INCIDENTI PER LA SICUREZZA DELLE INFORMAZIONI

1. Il Fornitore dovrà preparare e mantenere un piano e un programma di risposta agli incidenti contenente le procedure e le indicazioni da seguire in caso di incidente relativo alla sicurezza dell'infrastruttura informatica del Fornitore, documentando i passaggi necessari ei canali di comunicazione da seguire.
2. Il Fornitore dovrà garantire che le indicazioni incorporino procedure appropriate per notificare a PG e ad altre parti interessate necessarie, tempestivamente, se viene determinato che un Incidente di sicurezza ha causato una violazione della sicurezza che coinvolge le Informazioni o i Dati personali del Cliente.
3. Il Fornitore informerà il Cliente della debolezza individuata nel sistema e nei servizi che influiscono sulla sicurezza delle Informazioni e dei Dati personali del Cliente.

13. ASPETTI DELLA SICUREZZA DELLE INFORMAZIONI DELLA GESTIONE DELLA CONTINUITÀ AZIENDALE

1. Il Fornitore svilupperà e manterrà analisi dell'impatto sulla continuità operativa e piani di ripristino di emergenza, progettati per prevenire la perdita di informazioni sui clienti e dati personali, nonché per mantenere la fornitura dei Servizi da parte del Fornitore con interruzioni minime. Ciascun piano dettaglia le misure per supportare l'efficace ripristino dei servizi, per riprendere le operazioni il prima possibile dopo un'emergenza.
2. Il Fornitore dovrà condurre test periodici delle funzioni aziendali più critiche, per garantire che queste siano prontamente disponibili in caso di disastro dichiarato.
3. Il fornitore dovrà implementare risorse logiche e fisiche ridondanti ove necessario per soddisfare i requisiti di disponibilità. I test periodici garantiscono un failover regolare.
4. Il Fornitore dovrà garantire che i backup vengano effettuati fuori sede, per supportare la recuperabilità dei sistemi del Fornitore in caso di disastro.

14. CONFORMITÀ

1. Il Fornitore dovrà garantire che i sistemi informativi del Fornitore siano conformi ai requisiti e alle politiche di sicurezza, alle leggi applicabili e ai requisiti normativi.
2. Il Fornitore dovrà implementare controlli di audit appropriati, limitando l'accesso a strumenti e sistemi prevenendo così l'uso improprio o la compromissione e garantendo che gli audit siano conformi alla Politica di sicurezza del Fornitore.

ALLEGATO 3

ELENCO DEI SUBPROCESSORI

(Nota interna: Nel caso in cui il Fornitore abbia già ingaggiato subappaltatori al momento della stipula del contratto occorre compilare tale allegato:
fornendo il nome del subappaltatore, il suo indirizzo e una descrizione dei servizi forniti dal subappaltatore in relazione al trattamento dei Dati Personali)
Il Cliente acconsente al fatto che il Fornitore assuma i seguenti sub-responsabili del trattamento:

Sub-responsabile del trattamento (denominazione legale completa)	Indirizzo/paese	Descrizione dei servizi forniti dai sub-incaricati

ALLEGATO 4

CLAUSOLE CONTRATTUALI STANDARD PER IL TRASFERIMENTO DI DATI PERSONALI DA UE A PAESI TERZI (TRASFERIMENTI DA TITOLARE A RESPONSABILE DEL TRASFERIMENTO)

Accordo sul trasferimento dei dati con le disposizioni del GDPR

Per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati

[DENOMINAZIONE DELLA PERSONA GIURIDICA DELL'ENTITÀ PG ESPORTANTEDATI PERSONALI]
[INDIRIZZO]
[TELEFONO]
[FAX]
[E-MAIL]
(l' **esportatore** di dati) e

[PERSONA GIURIDICA NOME DEL RESPONSABILE DEL TRATTAMENTO IL PERSONALEI DATI VENGONO TRASFERITI A]
[INDIRIZZO]
[TELEFONO]
[FAX]
[E-MAIL]
(l' **importatore** di dati)

ciascuno una “festa”; insieme “le parti”,

HANNO CONVENUTO le seguenti Clausole Contrattuali (le Clausole) al fine di apportare adeguate garanzie rispetto alla tutela della privacy e dei diritti e delle libertà fondamentali delle persone per il trasferimento da parte dell'esportatore di dati all'importatore di dati dei dati personali di cui all'Allegato 1 .

CLAUSOLA 1

Definizioni

Ai fini delle Clausole:

(a) "dati personali", "categorie speciali di dati", "trattamento/trattamento", "responsabile del trattamento", "responsabile del trattamento", "interessato" e "autorità di controllo" hanno lo stesso significato della normativa applicabile in materia di protezione dei dati;

(b) 'l'esportatore di dati' indica il titolare del trattamento che trasferisce i dati personali;

(c) 'l'importatore di dati' indica il responsabile del trattamento che accetta di ricevere dall'esportatore di dati i dati personali destinati al trattamento per suo conto dopo il trasferimento secondo le sue istruzioni e i termini delle Clausole e che non è soggetto al sistema di un paese terzo che garantisca un'adeguata protezione ai sensi della legge applicabile in materia di protezione dei dati;

(d) 'il sub-responsabile' indica qualsiasi responsabile incaricato dall'importatore di dati o da qualsiasi altro sub-responsabile dell'importatore di dati che accetta di ricevere dall'importatore di dati o da qualsiasi altro sub-responsabile dell'importatore di dati dati personali destinati esclusivamente alle attività di trattamento da svolgere per conto dell'esportatore dei dati dopo il trasferimento secondo le sue istruzioni, i termini delle Clausole e i termini del subappalto scritto;

(e) 'normativa applicabile in materia di protezione dei dati' indica la Direttiva 95/46/CE e qualsiasi normativa e/o regolamento di attuazione o emanazione in applicazione di essa, o che modifichi, sostituisca, reintroduca o consolida una di essa (compreso il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)) , e tutte le altre leggi applicabili relative al trattamento dei dati personali che possono esistere in qualsiasi giurisdizione pertinente, comprese, ove applicabili, le linee guida e i codici di condotta emanati dalle autorità di controllo, la legislazione a tutela dei diritti e delle libertà fondamentali delle persone e, in in particolare, il loro diritto alla riservatezza rispetto al trattamento dei dati personali applicabile a un titolare del trattamento nello Stato membro in cui è stabilito l'esportatore di dati;

(f) per "misure di sicurezza tecniche e organizzative" si intendono quelle misure volte a proteggere i dati personali dalla distruzione accidentale o illecita o dalla perdita, alterazione accidentale, divulgazione o accesso non autorizzati, in particolare laddove il trattamento comporti la trasmissione di dati su una rete, e contro ogni altro illecito forme di trattamento.

CLAUSOLA 2

Dettagli del trasferimento

Gli estremi del conferimento ed in particolare le categorie particolari di dati personali ove applicabili sono specificati nell'Allegato 1 che forma parte integrante delle Clausole.

CLAUSOLA 3

Clausola di terzo beneficiario

1. L'interessato può far valere nei confronti dell'esportatore di dati la presente Clausola, le Clausole da 4(b) a (i), le Clausole 5 da (a) a (e) e da (g) a (j), le Clausole 6(1) e (2) , Clausola 7, Clausola 8(2) e Clausole da 9 a 12 come terzo beneficiario.
2. L'interessato può far valere nei confronti dell'importatore di dati la presente Clausola, le Clausole da (a) a (e) e (g), le Clausole 6, le Clausole 7, le Clausole 8(2) e le Clausole da 9 a 15 nei casi in cui l'esportatore di dati ha di fatto è scomparso o ha cessato di esistere giuridicamente a meno che l'entità successore non abbia assunto tutti gli obblighi legali dell'esportatore di dati per contratto o per effetto di legge, in conseguenza dei quali assume i diritti e gli obblighi dell'esportatore di dati, in cui nel caso in cui l'interessato possa opporsi a tale soggetto.
3. L'interessato può far valere nei confronti del sub-responsabile del trattamento la presente Clausola, le Clausole da (a) a (e) e (g), le Clausole 6, le Clausole 7, le Clausole 8(2) e le Clausole da 9 a 15 nei casi in cui sia l'esportatore di dati che l'importatore di dati è di fatto scomparso o ha cessato di esistere legalmente o è diventato insolvente, a meno che qualsiasi ente successore non abbia assunto tutti gli obblighi legali dell'esportatore di dati per contratto o per effetto di legge in conseguenza dei quali assume i diritti e gli obblighi dell'esportatore di dati, nel qual caso l'interessato può farli valere nei confronti di tale entità. Tale responsabilità di terzi del sub-responsabile del trattamento sarà limitata alle proprie operazioni di trattamento ai sensi delle Clausole.
4. Le parti non si oppongono al fatto che un interessato sia rappresentato da un'associazione o altro organismo se l'interessato lo desidera espressamente e se consentito dal diritto nazionale.

CLAUSOLA 4

Obblighi dell'esportatore di dati

L'esportatore di dati accetta e garantisce:

(a) che il trattamento, compreso il trasferimento stesso, dei dati personali è stato e continuerà ad essere effettuato in conformità con le pertinenti disposizioni della normativa applicabile in materia di protezione dei dati (e, ove applicabile, è stato notificato alle autorità competenti del Membro Stato in cui è

stabilito l'esportatore di dati) e non viola le pertinenti disposizioni di tale Stato;

(b) di aver istruito e per tutta la durata dei servizi di trattamento dei dati personali incaricherà l'importatore di dati di trattare i dati personali trasferiti solo sui dati per conto dell'esportatore e in conformità con la legge sulla protezione dei dati applicabile e le Clausole;

(c) che l'importatore di dati fornisca sufficienti garanzie nel rispetto delle misure di sicurezza tecniche e organizzative specificate nell'allegato 2 al presente contratto;

(d) che, previa valutazione dei requisiti della normativa applicabile in materia di protezione dei dati, le misure di sicurezza siano idonee a proteggere i dati personali dalla distruzione accidentale o illecita o dalla perdita accidentale, dall'alterazione, dalla divulgazione o dall'accesso non autorizzati, in particolare laddove il trattamento comporti la trasmissione di dati su un rete, e contro ogni altra forma illecita di trattamento, e che tali misure garantiscono un livello di sicurezza adeguato ai rischi presentati dal trattamento e alla natura dei dati da proteggere, tenuto conto dello stato della tecnica e del costo della loro implementazione;

(e) che assicurerà il rispetto delle misure di sicurezza;

(f) che, qualora il trasferimento riguardi categorie particolari di dati, l'interessato è stato informato o sarà informato prima o non appena possibile dopo il trasferimento che i suoi dati potrebbero essere trasmessi a un paese terzo che non fornisce adeguata protezione ai sensi dell'art. la legge sulla protezione dei dati applicabile;

(g) inoltrare qualsiasi notifica ricevuta dall'importatore di dati o da qualsiasi subincaricato del trattamento ai sensi della clausola 5(b) e della clausola 8(3) all'autorità di controllo della protezione dei dati se l'esportatore di dati decide di continuare il trasferimento o revocare la sospensione;

(h) di mettere a disposizione degli interessati, previa richiesta, copia delle Clausole, ad eccezione dell'Allegato 2, e una sintetica descrizione delle misure di sicurezza, nonché copia dell'eventuale contratto di servizi di subelaborazione da stipulare ai sensi dell'art. le Clausole, a meno che le Clausole o il contratto non contengano informazioni commerciali, nel qual caso può rimuovere tali informazioni commerciali;

(i) che, in caso di subtrattamento, l'attività di trattamento sia svolta ai sensi della Clausola 11 da un sub-responsabile che fornisce almeno lo stesso livello di protezione dei dati personali e dei diritti dell'interessato dell'importatore di dati ai sensi delle Clausole; e

(j) che garantirà il rispetto della clausola 4 da (a) a (i).

CLAUSOLA 5

Obblighi dell'importatore di dati

L'importatore di dati accetta e garantisce:

(a) trattare i dati personali solo per conto dell'esportatore dei dati e nel rispetto delle sue istruzioni e delle Clausole; se non può fornire tale adempimento per qualsiasi motivo, si impegna ad informare tempestivamente l'esportatore di dati della propria impossibilità a ottemperare, nel qual caso l'esportatore di dati ha il diritto di sospendere il trasferimento dei dati e/o risolvere il contratto;

(b) che non ha motivo di ritenere che la normativa ad essa applicabile le impedisca di adempiere alle istruzioni ricevute dall'esportatore di dati e ai suoi obblighi contrattuali e che in caso di modifica di tale normativa che possa avere un effetto negativo sostanziale sulle garanzie e sugli obblighi previsti dalle Clausole, comunicherà tempestivamente la modifica all'esportatore di dati non appena ne avrà conoscenza, nel qual caso l'esportatore di dati potrà sospendere il trasferimento dei dati e/o risolvere il contratto;

(c) di aver adottato le misure di sicurezza tecniche e organizzative di cui all'allegato 2 prima del trattamento dei dati personali conferiti;

(d) che informerà tempestivamente l'esportatore dei dati in merito a:

(i) qualsiasi richiesta legalmente vincolante di divulgazione dei dati personali da parte di un'autorità di contrasto, salvo diversa proibizione, come un divieto ai sensi del diritto penale di preservare la riservatezza di un'indagine delle forze dell'ordine,

(ii) qualsiasi accesso accidentale o non autorizzato, e

(e) qualsiasi richiesta pervenuta direttamente dagli interessati senza dare risposta a tale richiesta, salvo diversa autorizzazione a farlo; trattare tempestivamente e correttamente tutte le richieste dell'esportatore di dati relative al trattamento dei dati personali oggetto del trasferimento e attenersi al parere dell'autorità di controllo in merito al trattamento dei dati trasferiti;

(f) su richiesta dell'esportatore di dati di sottoporre le proprie strutture informatiche alla verifica delle attività di trattamento di cui alle Clausole che devono essere svolte dall'esportatore di dati o da un organismo di controllo composto da membri indipendenti e in possesso delle qualifiche professionali richieste vincolate da un obbligo di riservatezza, scelto dall'esportatore dei dati, ove previsto, d'intesa con l'autorità di controllo;

(g) mettere a disposizione dell'interessato su richiesta copia delle Clausole, o di qualsiasi contratto in essere per subtrattamenti, a meno che le Clausole o il contratto non contengano informazioni commerciali, nel qual caso può rimuovere tali informazioni commerciali, ad eccezione dell'Allegato 2 che deve essere sostituito da una descrizione sommaria delle misure di sicurezza nei casi in cui l'interessato non è in grado di ottenere copia dall'esportatore dei dati;

(h) che, in caso di subtrattamento, ha preventivamente informato l'esportatore dei dati e ottenuto il suo preventivo consenso scritto;

(i) che i servizi di elaborazione da parte del sub-responsabile del trattamento saranno effettuati in conformità con la Clausola 11;

(j) di inviare tempestivamente all'esportatore dei dati copia degli eventuali accordi di sub-responsabile stipulati ai sensi delle Clausole.

CLAUSOLA 6

Responsabilità

1. Le parti convengono che qualsiasi interessato, che abbia subito un danno a seguito della violazione degli obblighi di cui all'articolo 3 o all'articolo 11 da parte di qualsiasi parte o sub-responsabile del trattamento, ha diritto a ricevere un risarcimento dall'esportatore dei dati per il danno subito.
2. Se un interessato non è in grado di presentare una richiesta di risarcimento ai sensi del paragrafo 1 nei confronti dell'esportatore di dati, a causa di una violazione da parte dell'importatore di dati o del suo sub-responsabile del trattamento di uno qualsiasi degli obblighi di cui alla clausola 3 o alla clausola 11, poiché l'esportatore di dati è di fatto scomparso o ha cessato di esistere per legge o è diventato insolvente, l'importatore di dati accetta che l'interessato possa presentare un reclamo contro l'importatore di dati come se fosse l'esportatore di dati, a meno che l'entità successore non abbia assunto l'intera obblighi legali dell'esportatore di dati per contratto o per effetto di legge, nel qual caso l'interessato può far valere i propri diritti nei confronti di tale entità.

   L'importatore di dati non può fare affidamento su una violazione da parte di un sub-incaricato dei propri obblighi al fine di evitare le proprie responsabilità.
3. Se un interessato non è in grado di agire contro l'esportatore di dati o l'importatore di dati di cui ai paragrafi 1 e 2, a causa di una violazione da parte del sub-responsabile del trattamento di uno qualsiasi degli obblighi di cui alla clausola 3 o alla clausola 11 perché sia l'esportatore di dati che l'importatore di dati sono di fatto scomparsi o hanno cessato di esistere legalmente o sono diventati insolventi, il sub-responsabile accetta che l'interessato possa presentare un reclamo contro il sub-responsabile del trattamento in relazione ai propri trattamenti ai sensi delle Clausole come se era l'esportatore di dati o l'importatore di dati, a meno che qualsiasi entità successore abbia assunto tutti gli

obblighi legali dell'esportatore di dati o dell'importatore di dati per contratto o per effetto di legge, nel qual caso l'interessato può far valere i propri diritti nei confronti di tale entità. La responsabilità del sub-responsabile del trattamento è limitata alle proprie operazioni di trattamento ai sensi delle Clausole.

4. Le parti convengono che se una parte è ritenuta responsabile per una violazione delle Clausole commessa dall'altra parte, quest'ultima, nella misura in cui è responsabile, risarcirà la prima parte per qualsiasi costo, onere, danno, spesa o perdita ha sostenuto. L'indennità è subordinata a:
   (a) l'esportatore di dati notifica tempestivamente all'importatore di dati un reclamo; e
   (b) all'importatore di dati è data la possibilità di collaborare con l'esportatore di dati nella difesa e nella composizione del reclamo.

CLAUSOLA 7

Mediazione e giurisdizione

1. L'importatore di dati accetta che se l'interessato fa valere nei suoi confronti diritti di beneficiario di terzi e/o chiede il risarcimento dei danni ai sensi delle Clausole, l'importatore di dati accetterà la decisione dell'interessato:
   (a) deferire la controversia alla mediazione, da parte di un soggetto indipendente o, ove applicabile, dall'autorità di controllo;
   (b) deferire la controversia ai giudici dello Stato membro in cui è stabilito l'esportatore di dati.
2. Le parti convengono che la scelta operata dall'interessato non pregiudicherà i suoi diritti sostanziali o procedurali di ricorrere ai rimedi in conformità con altre disposizioni di diritto nazionale o internazionale.

CLAUSOLA 8

Collaborazione con le autorità di vigilanza

1. L'esportatore di dati si impegna a depositare una copia del presente contratto presso l'autorità di controllo se lo richiede o se tale deposito è richiesto dalla legge sulla protezione dei dati applicabile.
2. Le parti convengono che l'autorità di controllo ha il diritto di condurre un audit dell'importatore di dati, e di qualsiasi subincaricato, che abbia lo stesso scopo ed è soggetto alle stesse condizioni che si applicherebbero a un audit dell'esportatore di dati ai sensi dei dati applicabili legge di protezione.
3. L'importatore di dati informa tempestivamente l'esportatore di dati dell'esistenza di una normativa ad esso applicabile o di qualsiasi subincaricato che impedisca lo svolgimento di una verifica dell'importatore di dati, o di qualsiasi subincaricato, ai sensi del paragrafo 2. In tal caso, l'esportatore di dati ha il diritto di adottare le misure previste nella clausola 5 (b).

CLAUSOLA 9

Legge governativa

Le clausole sono disciplinate dalla legge dello Stato membro in cui è stabilito l'esportatore di dati.

CLAUSOLA 10

Variazione del contratto

1. Le parti si impegnano a non variare o modificare le Clausole. Ciò non impedisce alle parti di aggiungere clausole su questioni relative all'attività ove richiesto, purché non siano in contraddizione con le clausole.
2. Come nuove disposizioni/clausole sono state aggiunte le seguenti clausole commerciali:
   (a) Clausola 13 (Ulteriori obblighi dell'importatore di dati);
   (b) Clausola 14 (Correzione, cancellazione e blocco dei dati); e
   (c) Clausola 15 (Diritti degli interessati).

CLAUSOLA 11

Sottoelaborazione

1. L'importatore di dati non subappalta alcuna delle sue operazioni di trattamento eseguite per conto dell'esportatore di dati ai sensi delle Clausole senza il previo consenso scritto dell'esportatore di dati. Se l'importatore di dati subappalta i propri obblighi ai sensi delle clausole, con il consenso dell'esportatore di dati, lo fa solo mediante un accordo scritto con il sub-responsabile del trattamento che imponga al sub-responsabile gli stessi obblighi imposti all'importatore di dati ai sensi del Clausole. Qualora il sub-responsabile del trattamento non adempia ai propri obblighi in materia di protezione dei dati ai sensi di tale accordo scritto, l'importatore di dati resta pienamente responsabile nei confronti dell'esportatore di dati per l'adempimento degli obblighi del sub-responsabile del trattamento ai sensi di tale accordo.
2. Il previo contratto scritto tra l'importatore di dati e il sub-responsabile del trattamento prevede anche una clausola di terzo beneficiario come previsto dalla clausola 3 per i casi in cui l'interessato non è in grado di proporre la domanda di risarcimento di cui al comma 1 della clausola 6 contro l'esportatore di dati o i dati

   importatore perché sono di fatto scomparsi o hanno cessato di esistere legalmente o sono diventati insolventi e nessun ente successore ha assunto tutti gli obblighi legali dell'esportatore o importatore di dati per contratto o per effetto di legge. Tale responsabilità di terzi del sub-responsabile del trattamento sarà limitata alle proprie operazioni di trattamento ai sensi delle Clausole.
3. Le disposizioni relative agli aspetti di protezione dei dati per il subtrattamento del contratto di cui al comma 1 sono disciplinate dalla legge dello Stato membro in cui è stabilito l'esportatore dei dati.
4. L'esportatore di dati conserva un elenco degli accordi di subelaborazione conclusi ai sensi delle clausole e notificati dall'importatore di dati ai sensi della clausola 5 (j), che deve essere aggiornato almeno una volta all'anno. L'elenco è a disposizione dell'autorità di controllo della protezione dei dati dell'esportatore di dati.

CLAUSOLA 12

Obbligo dopo la cessazione dei servizi di trattamento dei dati personali

1. Le parti convengono che alla cessazione della prestazione dei servizi di elaborazione dati, l'importatore di dati e il subincaricato, a scelta dell'esportatore di dati, restituiscano tutti i dati personali trasferiti e le copie degli stessi all'esportatore di dati o distruggano tutti i dati personali e attestare all'esportatore di dati di averlo fatto, a meno che la legislazione europea o degli Stati membri imposta all'importatore di dati gli impedisca di restituire o distruggere, in tutto o in parte, i dati personali trasferiti. In tal caso, l'importatore di dati garantisce che garantirà la riservatezza dei dati personali trasferiti e non tratterà più attivamente i dati personali trasferiti.
2. L'importatore di dati e il sub-responsabile garantiscono che, su richiesta dell'esportatore e/o dell'autorità di controllo, sottoporrà le proprie strutture informatiche ad una verifica delle misure di cui al comma 1.

ALLEGATO 4.A

CLAUSOLE CONTRATTUALI STANDARD "APPENDICE MISURE COMPLEMENTARI"

SFONDO

1. Nella sentenza C-311/18 (Schrems II) la Corte di giustizia dell'Unione europea (CGUE) ha indicato che i titolari del trattamento o gli incaricati del trattamento, in qualità di esportatori di dati, sono responsabili della verifica, caso per caso e, ove opportuno, in collaborazione con l'importatore di dati nel paese terzo, se la legge o la prassi del paese terzo pregiudica l'efficacia delle garanzie appropriate contenute nelle Standard Contractual Clauses (SCC). In questi casi, la CGUE lascia ancora aperta la possibilità agli esportatori e agli importatori di dati di attuare misure supplementari che colmino eventuali (eventuali) lacune nella protezione e la portino al livello richiesto dal diritto dell'UE.
2. La presente appendice fornisce ulteriori misure integrative, attingendo alle raccomandazioni contenute nelle Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello UE di protezione dei dati personali, adottate dal Comitato europeo per la protezione dei dati il 10 novembre 2020.

TERMINI CONCORDATI

1. La presente appendice fa parte delle clausole contrattuali standard da titolare a responsabile del trattamento ai sensi della decisione 2010/87/UE della Commissione UE nell'allegato 4.
2. In caso di conflitto tra:
   (a) Le clausole della presente Appendice 4.A; e
   (b) Le Clausole adottate dalla Commissione Europea con Decisione della Commissione 2010/87/UE,

le Clausole descritte nella Clausola 2(b) della presente Appendice avranno la precedenza.

3. Per quanto riguarda l'eventuale accesso ai dati personali trasferiti da parte delle pubbliche autorità, l'importatore di dati garantisce e si impegna a:
   (a) esamina, secondo le leggi del paese di destinazione, la legittimità di qualsiasi richiesta di divulgazione dei dati personali trasferiti a un'autorità pubblica, in particolare se rimane nell'ambito dei poteri conferiti all'autorità pubblica richiedente, e ad esaurire tutti i rimedi disponibili di impugnare la richiesta se, dopo un'attenta valutazione, conclude che le leggi del paese di destinazione sussistono motivi per farlo. Nell'impugnare una richiesta, l'importatore di dati chiede provvedimenti cautelari volti a sospendere gli effetti della richiesta fino a quando il giudice non si sia pronunciato nel merito. Non divulga i dati personali trasferiti richiesti a meno che e fino a quando non sia richiesto dalla legge o dalle norme procedurali applicabili;
   (b) documenta l'accertamento giuridico effettuato sub a), nonché l'eventuale impugnazione della richiesta di divulgazione e, nei limiti consentiti dalla normativa del Paese di destinazione, la mette a disposizione dell'esportatore dei dati. Lo mette inoltre a disposizione dell'autorità di controllo competente su richiesta;
   (c) fornisce la quantità minima di informazioni consentita nel rispondere a una richiesta di divulgazione dei dati personali trasferiti, sulla base di un'interpretazione ragionevole della richiesta;
   (d) informa l'autorità pubblica richiedente dell'eventuale incompatibilità della richiesta con le garanzie contenute nelle Clausole e del conseguente conflitto di obblighi per l'importatore di dati. L'importatore di dati deve altresì informare immediatamente l'esportatore di dati, per quanto possibile secondo le leggi del paese di destinazione;
   (e) documenta e registra le richieste di accesso ai dati trasferiti ricevute dalle autorità pubbliche e la risposta fornita nonché gli attori coinvolti. Tali registrazioni dovrebbero essere messe a disposizione dell'esportatore di dati, per quanto possibile in base alle leggi del paese di destinazione;
   (f) l'esportatore di dati può esercitare il proprio potere di richiedere che l'importatore di dati sottoponga le sue strutture di elaborazione e altra documentazione e file a audit o ispezione ai sensi della clausola 5(f) delle clausole dando un preavviso di 12 ore all'importatore di dati. L'importatore di dati garantisce che l'esportatore di dati sia in grado di verificare se i dati personali trasferiti sono stati divulgati alle autorità pubbliche ea quali condizioni sono stati divulgati. In particolare, i registri di accesso e altre tracce simili devono essere a prova di manomissione in modo che i revisori siano in grado di trovare prove della divulgazione. I registri degli accessi e altri percorsi simili devono inoltre distinguere tra accessi dovuti a normali operazioni commerciali e accessi dovuti a ordini o richieste di accesso. Nell'adempimento dei propri obblighi ai sensi della presente clausola, l'importatore di dati coopererà in ogni circostanza con l'esportatore di dati e l'autorità di controllo competente in modo tempestivo;
   (g) compirà ogni ragionevole sforzo per monitorare eventuali sviluppi legali o politici che potrebbero comportare la sua incapacità di adempiere ai propri obblighi ai sensi delle Clausole. In particolare, l'importatore di dati compie ogni ragionevole sforzo per informare l'esportatore di dati degli sviluppi giuridici o politici prima della loro attuazione e, ove possibile, prima che sia concesso l'accesso ai dati personali trasferiti;
   (h) non ha creato intenzionalmente backdoor o programmi simili che potrebbero essere utilizzati dalle autorità pubbliche per accedere a uno o entrambi i seguenti elementi:
   (i) il/i sistema/i utilizzato/i dall'importatore di dati per il trattamento dei dati personali trasferiti;
   (ii) gli stessi dati personali trasferiti;
   (i) non ha creato o modificato di proposito i propri processi aziendali in modo da facilitare l'accesso a tali dati o sistemi personali da parte delle autorità pubbliche; e
   (j) per quanto a sua conoscenza, la legge nazionale o la politica del governo applicabile all'importatore di dati non richiedono all'importatore di dati di eseguire una o entrambe le seguenti operazioni:
   (i) creare o mantenere backdoor o per facilitare l'accesso ai dati o ai sistemi personali trasferiti da parte delle autorità pubbliche;
   (ii) essere in possesso o consegnare la chiave di crittografia.

Per conto dell'esportatore di dati:	**Per conto dell'importatore di dati:**
Nome (scritto per intero):	Nome (scritto per intero):
Posizione:	Posizione:
Data:	Data:
Firma:	Firma:

Nome (scritto per intero):	Nome (scritto per intero):
Posizione:	Posizione:
Data:	Data:
Firma:	Firma: