CLAUSOLE CONTRATTUALI TRA IL TITOLARE ED IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28 del Regolamento UE 2016/679

TRA

Il **Ministero del Lavoro e delle Politiche Sociali** (di seguito anche "MLPS"), C.F./P.IVA ……., con sede legale in ……, in persona del suo legale rappresentante ……, in qualità di Titolare del trattamento dei dati personali, ai sensi dell'art. 4 par. 7 del Regolamento (UE) 2016/679

E

la società …… con sede legale in ……..nella Via……., P.IVA/C.F ……..(*di seguito: "Fornitore" o "Responsabile del trattamento*"), nella persona del suo legale rappresentante……, **congiuntamente indicate come "Parti".**

Premesso che

- Il MLPS, previo espletamento della procedura di gara in oggetto, ha affidato al Fornitore, giusta Deliberazione n……del ……, il servizio di ……; pertanto il Fornitore dovrà/potrà effettuare operazioni di trattamento dei Dati Personali per conto dell'Azienda;
- Il MLPS svolge il ruolo di Titolare del trattamento in relazione ai Dati Personali dalla stessa trattati, stabilendo autonomamente le finalità, le modalità ed i mezzi del trattamento;
- il Fornitore è in possesso di adeguate competenze tecniche e *know-how* circa gli scopi e le modalità di trattamento dei Dati Personali, delle misure di sicurezza da adottare al fine di garantire la loro riservatezza, la completezza e l'integrità, nonché diretta e completa conoscenza delle norme che disciplinano la protezione degli stessi;
- con il presente atto - che costituisce parte integrante e sostanziale del contratto di cui sopra - Il MLPS, in qualità di Titolare del trattamento, intende nominare il Fornitore, che accetta, Responsabile del trattamento (di seguito anche "Fornitore"), ai sensi di quanto disposto dall'art. 28 del GDPR.
- con la sottoscrizione del presente documento le Parti intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali effettuato dal Fornitore/Responsabile del trattamento per conto del MLPS.

Tutto ciò premesso, alla luce di quanto precede, le Parti convengono e stipulano quanto segue:

Definizioni:

"GDPR":	il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
"Codice":	il D.Lgs. 196/2003 "Codice in materia dei dati personali" così come successivamente integrato e modificato (da ultimo dal D.Lgs 101/2018)
"Dato/i Personale/i"	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
"Categorie Particolari di Dati":	indica ogni Dato Personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
"Dati Giudiziari":	indica ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.
"Titolare del trattamento":	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
"Responsabile del trattamento":	chi effettua un trattamento dati per conto del titolare del trattamento (art. 28 GDPR)
"Trattamento":	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
"Comunicazione":	dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea,

	dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
"Interessato":	persona fisica cui si riferiscono i dati personali.
"Autorizzati":	le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile ai sensi dell'art. 29 del GDPR e dell'art. 2 *quaterdecies* del Codice.
"Subfornitore/Sub-Responsabile":	indica qualsiasi soggetto, persona fisica o giuridica, a cui il Responsabile ricorra per l'esecuzione di specifiche attività di Trattamento per conto del Titolare a cui sono imposti gli stessi obblighi del Responsabile.
"Terze Parti o Terzi":	indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non siano l'interessato, il Titolare, il Responsabile e gli incaricati autorizzati al trattamento dei Dati Personali sotto l'autorità diretta del titolare o del responsabile.
"Gruppo di Lavoro Articolo 29" (WP):	indica il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE.
"Comitato Europeo per la protezione dei dati":	*European Data Protection Board* indica l'organismo dell'Unione Europea dotato di personalità giuridica istituito ai sensi degli artt. 68 e ss. del GDPR, che ha sostituito il Gruppo di lavoro articolo 29 (Working Party article 29 o WP29), gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.
"Autorità di Controllo":	indica il Garante per la protezione dei Dati Personali.
"Accordo di trasferimento dei dati":	indica ogni accordo stipulato tra le Parti e finalizzato al trasferimento legittimo dei Dati Personali.

Clausole contrattuali tipo

SEZIONE I

Clausola 1
Scopo e ambito di applicazione

Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati.
I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679.
Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.
Gli allegati da I a IV costituiscono parte integrante delle clausole.
Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del Regolamento (UE) 2016/679 e/o del Regolamento (UE) 2018/1725.
Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del Regolamento (UE) 2016/679 o del Regolamento (UE) 2018/1725.

Clausola 2
Invariabilità delle clausole

Le Parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.
Ciò non impedisce alle Parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3
Interpretazione

Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679.
Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679 o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4
Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le Parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5
Clausola di adesione successiva

a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le Parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di Responsabile del trattamento, compilando gli allegati e firmando l'allegato I.
b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un Responsabile del trattamento, conformemente alla sua designazione nell'allegato I.
c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II

OBBLIGHI DELLE PARTI

Clausola 6
Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7
Obblighi delle Parti

7.1 Istruzioni

Il Responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento. In tal caso, il Responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.
Il Responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il Regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2 Limitazione delle finalità

Il Responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3 Durata del trattamento dei dati personali

Il Responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4 Sicurezza del trattamento

Il Responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.
Il Responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5 Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»), il Responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6 Documentazione e rispetto

Le Parti devono essere in grado di dimostrare il rispetto delle presenti clausole.
Il Responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
Il Responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal Regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il Responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento.
Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.
Su richiesta, le Parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7 Ricorso a sub-responsabili del trattamento

a) Il Responsabile del trattamento non può sub-contrattare a un sub-Responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il Responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno 30 giorni prima di ricorrere al sub-Responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere

in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le Parti tengono aggiornato tale allegato.

b) Qualora il Responsabile del trattamento ricorra a un sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del Responsabile del trattamento), stipula un contratto che impone al sub-Responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al Responsabile del trattamento conformemente alle presenti clausole. Il Responsabile del trattamento si assicura che il sub-Responsabile del trattamento rispetti gli obblighi cui il Responsabile del trattamento è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679.
c) Su richiesta del titolare del trattamento, il Responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-Responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
d) Il Responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-Responsabile del trattamento derivanti dal contratto che questi ha stipulato con il Responsabile del trattamento. Il Responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-Responsabile del trattamento, degli obblighi contrattuali.
e) Il Responsabile del trattamento concorda con il sub-Responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il Responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-Responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8 Trasferimenti internazionali

Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento, e nel rispetto del capo V del Regolamento (UE) 2016/679.
Il titolare del trattamento conviene che, qualora il Responsabile del trattamento ricorra a un sub-Responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del Regolamento (UE) 2016/679, il Responsabile del trattamento e il sub-Responsabile del trattamento possono garantire il rispetto del capo V del Regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

7.9 Attribuzione delle funzioni di amministratore di sistema

Il Responsabile del trattamento deve assicurare, se del caso, la puntuale adozione delle misure di cui al Provvedimento dell'Autorità Garante per la protezione dei dati personali "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 e successive modifiche ed integrazioni.

In particolare, il Responsabile deve:

a) Provvedere alla designazione dei propri amministratori di sistema in forma scritta su base individuale, con elencazione analitica dell'ambito di operatività consentita in base al profilo di autorizzazione assegnata;
b) Stilare la lista degli amministratori di sistema e provvedere al relativo periodico aggiornamento. Tale lista dovrà includere gli estremi identificativi delle persone fisiche amministratori di sistema con l'elenco delle funzioni ad essi attribuite;
c) Fornire tempestivamente la lista aggiornata degli amministratori di sistema ogni qualvolta il Titolare ne faccia richiesta, anche tramite propri delegati e, in ogni caso, almeno una volta all'anno;
d) Garantire l'effettuazione di una verifica almeno annuale sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste da vigente normativa per i trattamenti di Dati Personali;
e) Adottare, relativamente ai software utilizzati, sistemi idonei alla registrazione degli accessi logici (log applicativi) da parte degli utenti e degli amministratori di sistema. Le registrazioni devono:
    - avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste;
    - comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;
    - essere conservate per un congruo periodo, comunque non inferiore ad un anno e rese disponibili tempestivamente al Titolare, ogniqualvolta questi ne faccia richiesta, anche a mezzo di propri delegati.

Clausola 8
Assistenza al titolare del trattamento

a) Il Responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

b) Il Responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il Responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.
c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il Responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del Responsabile del trattamento:

1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA ai sensi dell'art. 35 del Regolamento (UE) 2016/679) qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
2) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
4) gli obblighi di cui all'articolo 32 Regolamento (UE) 2016/679.

d) Le Parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il Responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9
Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il Responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.

9.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il Responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del Regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2) le probabili conseguenze della violazione dei dati personali;
3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e

le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del Regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2 Violazione riguardante dati trattati dal Responsabile del trattamento

In caso di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
Le Parti stabiliscono nell'allegato III tutti gli altri elementi che il Responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679.

SEZIONE III
DISPOSIZIONI FINALI

Clausola 10
Inosservanza delle clausole e risoluzione

a) Fatte salve le disposizioni del Regolamento (UE) 2016/679, qualora il Responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al Responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il Responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

1) il trattamento dei dati personali da parte del Responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
2) il Responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;

3) il Responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del Regolamento (UE) 2016/679.

c) Il Responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

d) Dopo la risoluzione del contratto il Responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I
[compilazione a cura del MLPS]

Elenco delle Parti

1. **Titolare/i del trattamento:** [Identità e dati di contatto del/dei titolari del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

Ministero del Lavoro e delle Politiche Sociali

Legale rappresentante: Dott. ……..
Designato al trattamento (esercente le funzioni di Titolare): **Dott. ……..**

email: …….
pec: …….

Responsabile della protezione dei dati: NB CONSULTING (Ing. Nicola Barberini)
Email: dpo@lavoro.gov.it
Pec: dpo@pec.lavoro.gov.it

Firma e data di adesione: ……

Responsabile/i del trattamento [Identità e dati di contatto del/dei responsabili del trattamento e, ove applicabile, del suo/loro responsabile della protezione dei dati]

2. **Azienda:**
   Indirizzo:
   P.IVA/C.F

   E-mail:

Responsabile della protezione dei dati:

Firma e data di adesione: ……

ALLEGATO II

[compilazione a cura di MLPS]

DESCRIZIONE DEL TRATTAMENTO DEI DATI

Cod.	Voce	Descrizione
1	**AMBITO DI TRATTAMENTO**	
1.1	**Attività previste da contratto**	
1.2	**Finalità e base giuridica del trattamento dei dati**	
1.3	**Categorie di interessati**	
1.4	**Categorie di Dati Personali**	☐ **dati personali "comuni"**, in ossequio ai principi di cui all'art. 5 del GDPR, garantendo altresì la protezione dei dati per impostazione predefinita e fin dalla progettazione, ai sensi dell'art. 25 del GDPR (applicazione dei principi del Privacy by default e Privacy by design); ☐ **dati personali "appartenenti a categorie particolari"** (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), in ossequio ai principi di cui all'art. 5 del GDPR, garantendo altresì la protezione dei dati per impostazione predefinita e fin dalla progettazione, ai sensi dell'art. 25 del GDPR (applicazione dei principi del Privacy by default e Privacy by design); ☐ **dati soggetti a maggior tutela**: dati relativi alle infezioni da HIV, all'uso di sostanze stupefacenti, psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato, ad atti di violenza sessuale o di pedofilia, ai servizi offerti dai consultori familiari (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269; l. 6 febbraio 2006, n. 38; l. 5 giugno 1990, n. 135; d.P.R. 9 ottobre 1990, n. 309; l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349; l. 29 luglio 1975, n. 405)

		☐ **dati personali giudiziari relativi a "condanne penali e reati"**, in ossequio ai principi di cui all'art. 5 del GDPR, garantendo altresì la protezione dei dati per impostazione predefinita e fin dalla progettazione, ai sensi dell'art. 25 del GDPR (applicazione dei principi del Privacy by default e Privacy by design). Ulteriori dettagli:
1.5	**Categorie di Destinatari**	
1.6	**Durata del trattamento dei dati**	
1.7	**Durata della conservazione dei dati**	
2	**OPERAZIONI AUTORIZZATE DAL TITOLARE**	
2.1	**Raccolta**	SI
2.2	**Registrazione**	SI
2.3	**Organizzazione**	SI
2.4	**Strutturazione**	SI
2.5	**Conservazione**	SI
2.6	**Adattamento o Modifica**	SI
2.7	**Estrazione**	SI
2.8	**Consultazione**	SI
2.9	**Uso**	SI
2.10	**Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione**	SI
2.11	**Raffronto o Interconnessione**	SI
2.12	**Limitazione**	NO (salvo su richiesta del Titolare)
2.13	**Cancellazione**	NO (salvo su richiesta del Titolare)
2.14	**Trasferimento verso un paese terzo o una organizzazione internazionale**	NO (salvo su richiesta del Titolare)

ALLEGATO III

Misure tecniche e organizzative per garantire la sicurezza dei dati

[il presente allegato deve contenere i requisiti di sicurezza mandatori indicati nel capitolato e le misure opzionali indicate dal Partecipante]

Sono di seguito elencate le misure di sicurezza obbligatorie che il Titolare del trattamento prescrive al Responsabile del trattamento dei dati e le misure raccomandabili (opzionali), tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche (artt. 5-25-32 del Reg. UE 2016/679).

REQUISITI DI SICUREZZA "MANDATORI"
a) Politica interna definita dal Responsabile per la protezione dei dati personali, sicurezza delle informazioni e definizione di un modello organizzativo conforme al Regolamento UE 2016/679
b) Procedure interne del Responsabile per attribuzioni di compiti e funzioni (autorizzati e sub-responsabili del trattamento)
c) Misure tecniche ed organizzative per assicurare su base permanente la riservatezza, l'integrità, la disponibilità dei dati e la resilienza dei sistemi e dei servizi offerti dal Responsabile
d) Procedure per ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico su server fisici/virtuali del Responsabile
e) Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento posto in essere dal Responsabile
f) Misure di protezione dei dati trasmessi e conservati dal Responsabile (cifratura *in transit* e *at rest*)
g) Formazione periodica del personale del Responsabile, in materia di protezione dei dati personali
h) Misure per garantire la sicurezza fisica dei luoghi del Responsabile, in cui i dati personali del Titolare sono trattati
i) Misure di sicurezza per garantire la riservatezza delle comunicazioni da remoto (da e verso la rete del Titolare del trattamento)
j) Procedure per la gestione e governance della sicurezza informatica e della Cybersecurity sul software/prodotto/servizio offerto
k) Misure per garantire la tracciabilità degli accessi e delle operazioni effettuate sul software/prodotto/servizio offerto
l) Procedura per la gestione delle violazioni dei dati, ai sensi dell'art. 33 del Reg. UE 2016/679
m) Software Privacy *compliant*: Protezione dei dati personali trattati tramite il software/prodotto/servizio offerto, fin dalla progettazione e protezione per impostazione predefinita (*Privacy by design e by Default*) di cui all'art. 25 del Reg. UE 2016/679
n) Politica specifica per la password definita e documentata. La politica deve includere la lunghezza della password (almeno 8 caratteri), la complessità, il periodo di validità (non meno di 90 giorni) e il numero di tentativi di accesso non riusciti accettabili dal software/prodotto/servizio offerto.
o) Tecniche crittografiche applicate a livello database p) Tecniche crittografiche applicate sugli archivi di backup (anche se in cloud)
q) Test periodici OWASP o equivalenti, almeno annuali, sul software offerto

r) Test di Vulnerability Assessment e Penetration Test, almeno annuali, sul software/prodotto/servizio offerto. Consegna dei report al Titolare del trattamento con l'indicazione delle vulnerabilità riscontrate e delle azioni di risoluzione/mitigazione apportate.	
[compilazione a cura del Fornitore] **REQUISITI DI SICUREZZA "OPZIONALI"**	
s) Adesione a Codici di condotta di cui all'art. 40 del Reg. UE 2016/679	☐ applicata ☐ non applicata
t) Certificazioni della protezione dei dati di cui all'art. 42 del Reg. UE 2016/679 (certificazione di prodotto/processo/servizio)	☐ applicata ☐ non applicata
u) Elenco certificazioni possedute dal Fornitore a garanzia dei servizi offerti. E' possibile allegare ulteriore documentazione	□ ISO/IEC 27001 □ ISO/IEC 27017 □ ISO/IEC 27018 □ ISO/IEC 22301 □ ISO/IEC 25024 □ ISO/IEC 25012 □ altro…….. □ altro…….. □ altro…….. □ altro……..
v) Altro……	

Per i trasferimenti a sub-responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il sub-Responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

Descrizione delle misure tecniche e organizzative specifiche che il Responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento.

ALLEGATO IV
[compilazione a cura del Fornitore]

Elenco dei sub-responsabili del trattamento

NOTA ESPLICATIVA:
Il presente allegato deve essere compilato in caso di autorizzazione specifica di sub-responsabili del trattamento [clausola 7.7, lettera a).

Il Titolare del trattamento ha autorizzato il ricorso ai seguenti **sub-Responsabili** del trattamento:

[tabella da compilare per ciascun sub-responsabile autorizzato)

Ragione sociale	
Sede Legale	
P.IVA	
Descrizione del servizio/Attività di trattamento affidata al sub-fornitore	
Tipologia dati personali	□ Nessun dato personale □ Dati anonimi □ Dati personali di cui all'art. 6 del Reg. UE 2016/679 □ Dati personali di cui all'art. 9 del Reg. UE 2016/679 □ Dati personali soggetti a maggior tutela □ Dati personali di cui all'art. 10 del Reg. UE 2016/679
Dati di contatto del Referente	
Localizzazione Server Applicativo	□ U.E. [specificare Paese e Sede] [……] □ extra U.E. [specificare Paese e Sede] [……]
Localizzazione Server di database	□ U.E. [specificare Paese e Sede] [……] □ extra U.E. [specificare Paese e Sede] [……]

Localizzazione Server per disaster recovery e business continuity	□ U.E. [specificare Paese e Sede] [……..……] □ extra U.E. [specificare Paese e Sede] [……..……]
Localizzazione backup database/archivi	□ U.E. [specificare Paese e Sede] [……..……] □ extra U.E. [specificare Paese e Sede] [……..……]
Localizzazione archivio cartaceo	□ U.E. [specificare Paese e Sede] [……..……] □ extra U.E. [specificare Paese e Sede] [……..……]