ACCORDO PER IL TRATTAMENTO DEI DATI (DPA)

Tra il “CLIENTE” (di seguito "il titolare del trattamento")

da un lato,

e

STUDIO LAROCCA STP S.R.L. UNIPERSONALE (di seguito "il responsabile del trattamento")

d'altra parte.

I. Oggetto

Lo scopo di queste clausole è definire le condizioni alle quali il responsabile del trattamento (ai sensi e per gli effetti dell’art. 28 del GDPR) si impegna a svolgere, per conto del titolare del trattamento, le operazioni di trattamento dei dati personali definite di seguito. Nell'ambito del loro rapporto contrattuale esistente, le parti si impegnano a rispettare i regolamenti in vigore applicabili al trattamento dei dati personali e, in particolare, il Regolamento Europeo (UE) 2016/679 (GDPR) applicabile dal 25 maggio 2018 (di seguito "regolamento europeo sulla protezione dei dati").

II. Descrizione del/i trattamento/i

Il responsabile del trattamento è autorizzato, nell'ambito delle operazioni eseguite per conto del titolare del trattamento e oggetto della presente designazione, a trattare i dati personali necessari nonché a svolgere tutte le operazioni di trattamento necessarie con le eventuali specificazioni, come di seguito descritto.

Trattamento n.1: consulenza del lavoro (ivi compresi, ove previsti, i servizi di gestione informatizzata del personale)

Le finalità del trattamento sono riconducibili a:

- prestazione dei servizi di consulenza del lavoro e giuslavoristica;
- elaborazione presenze e Libro Unico del Lavoro (LUL);
- gestione paghe, calcolo contributi, emissione certificazione unica;
- archiviazione certificati, attestati, modulistica e documenti vari;
- esecuzione dei servizi di gestione (informatizzata e non) delle risorse umane;
- (eventualmente) gestione della piattaforma web utilizzata, anche affidandosi ad altro fornitore (in outsourcing);
- interventi tecnici, su richiesta, di assistenza e aggiornamento, nonché di supporto telematico (ove previsto).

I dati oggetto di trattamento sono:

- informazioni di identificazione personale o di contatto (recapiti);
- personali ed anche di natura “particolare” riconducibili allo stato generale di salute (assenze per malattia, maternità, infortunio o avviamento obbligatorio) o l’appartenenza a categorie protette (di cui alla Legge 68/99) e l’idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche) oltre che all'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale) o ad un partito politico o alla titolarità di cariche pubbliche elettive (permessi od aspettativa) ed alle convinzioni religiose (festività religiose fruibili per legge);
- personali (eventualmente) relativi a condanne penali e reati (art. 10 del GDPR) soltanto se legittimati da controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Le categorie di persone fisiche (interessati) sono:

- soggetti identificati (dipendenti o assimilati dei committenti/clienti) i cui dati personali sono oggetto di trattamento derivante dalla prestazione dell’attività lavorativa in materia di consulenza del lavoro e giuslavoristica;
- familiari (in caso, ad esempio, di assegni per il nucleo familiare, permessi per assistenza ai familiari, ecc.) degli stessi (sulla base del contratto di lavoro).

Il responsabile del trattamento ha facoltà di utilizzare gli asset tecnologici in sua dotazione (dispositivi elettronici come quelli di rete o servizi specifici ecc.) per lo svolgimento dei compiti assegnati e per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute dal Titolare. Per l'esecuzione del servizio oggetto del presente contratto, il titolare del trattamento fornisce al responsabile le ulteriori informazioni necessarie, unitamente alle istruzioni.

III. Durata del contratto

Il presente contratto entra in vigore dalla data di stipula e dura fino alla revoca ovvero alla cessazione del rapporto contrattuale esistente a cui è collegato.

IV. Obblighi del responsabile del trattamento nei confronti del titolare del trattamento

Il responsabile del trattamento si impegna a:

1. trattare i dati per i soli scopi del presente contratto di nomina del responsabile del trattamento.

2. elaborare i dati in conformità con le seguenti istruzioni del titolare del trattamento:
   - 2.1 solo in conformità con la legge applicabile;
   - 2.2 secondo quanto specificato nel rapporto contrattuale esistente in oggetto;
   - 2.3 come documentato ulteriormente in qualsiasi altra istruzione scritta fornita dal titolare del trattamento e sottoscritta da responsabile come costituente istruzioni per il trattamento dei dati personali in oggetto.

3. garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto.

4. garantire un livello di sicurezza (art. 32 del GDPR) adeguato ai rischi derivanti dalla perdita, anche accidentale, dei dati stessi, nonché dalla divulgazione o accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

5. soddisfare i requisiti di sicurezza volti ad assicurare su base permanente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché la resilienza dei sistemi e dei servizi (in particolare se riconducibili all'adozione di una piattaforma web),

- adottando adeguate misure tecniche (fisiche e logiche) ed organizzative di sicurezza intese quali precauzioni idonee ad evitare la perdita, l'accesso non autorizzato e la diffusione di documenti contenenti dati personali, o altri rischi per la sicurezza;
- installando sistemi per la protezione della rete volti a garantire un adeguato livello di sicurezza informatica;
- utilizzando tecniche di cifratura e di encryption dei dati, attraverso algoritmi riconosciuti (ad esempio, SHA-256);
- includendo misure di codifica in caso di scambio tra le parti di informazioni personali o protocolli che permettano di garantire la confidenzialità e l'autenticità delle informazioni scambiate (ad esempio, HTTPS);

e, in tutti i casi, implementando idonee procedure di salvataggio (backup) ed assicurando la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

6. garantire la cosiddetta business continuity e predisporre un'adeguata politica di archiviazione dei dati trattati (sia da un punto di vista di sicurezza elettronica sia da un punto di vista di sicurezza fisica),

- adottando un'archiviazione cartacea, per la quale sono previste procedure non automatizzate, al fine di consentirne l'accesso alle sole persone autorizzate: in particolare, tutti i dati di natura particolare (ove presenti) sono custoditi in locali ad accesso controllato, armadi ed armadietti e/o dispositivi equipollenti provvisti di serratura e chiusi a chiave;
- adottando un'archiviazione elettronica (digitalizzazione) per la quale sono previste procedure di controllo automatizzate, al fine di consentirne l'accesso mediante l'utilizzo di credenziali di autenticazione, che fanno riferimento ad uno specifico profilo di autorizzazione, costituite da una username e da una password.
- garantendo un servizio di smaltimento sicuro e certificato di tutti i dati, i documenti, i materiali e comunque tutte le informazioni - in qualsiasi forma o su qualsiasi supporto - ove non destinati all'archiviazione.

7. assicurare l'accesso ai soggetti interessati, adottando sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) agli archivi elettronici ovvero implementando idonee procedure di autenticazione al sistema (login e verifica utente con diritto di accesso) attraverso tecniche di strong authentication, garantendo altresì che le persone autorizzate a trattare dati personali nell'ambito del presente contratto:

- si impegnino a rispettare la riservatezza o siano comunque soggetti ad un appropriato obbligo legale di riservatezza;
- ricevano la formazione necessaria in materia di protezione dei dati personali.

8. tenere conto dei principi di protezione dei dati dalla progettazione e protezione dei dati per impostazione predefinita con riguardo a strumenti, prodotti, applicazioni o servizi.

9. nominare, ove se ne manifesti l'esigenza o l'opportunità, uno o più sub-responsabili del trattamento. Il responsabile del trattamento può utilizzare un altro responsabile del trattamento (in seguito denominato "il sub-responsabile" ovvero "il responsabile del trattamento successivo") per svolgere specifiche attività di trattamento. Il responsabile del trattamento successivo è tenuto a rispettare gli obblighi del presente contratto per conto e in conformità con le istruzioni del titolare del trattamento. È responsabilità del responsabile del trattamento iniziale assicurare che il responsabile del trattamento successivo offra le stesse garanzie sufficienti per l'attuazione di adeguate misure tecniche e organizzative per garantire che il trattamento soddisfi i requisiti del regolamento europeo sulla protezione dei dati. Se il responsabile del trattamento successivo non adempie ai propri obblighi di protezione dei dati, il responsabile del trattamento originario rimane pienamente responsabile nei confronti del titolare del trattamento delle prestazioni dell'altro responsabile del trattamento.

10. garantire l'esercizio dei diritti delle persone. Per quanto possibile, si deve assistere il titolare del trattamento nell'adempimento dell'obbligo di rispondere alle richieste di esercizio dei diritti dell'interessato: diritto di accesso, rettifica, cancellazione e opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto di non essere oggetto di una decisione individuale automatizzata (compresa la profilazione). Inoltre, il responsabile del trattamento deve informare tempestivamente il titolare del trattamento in merito a tali richieste, appena ricevute, contattandolo ai recapiti dallo stesso indicati.

11. notificare le violazioni dei dati personali. Il responsabile del trattamento notifica al titolare del trattamento ogni violazione dei dati personali entro un massimo di 36 ore dopo esserne venuto a conoscenza. Tale notifica deve essere accompagnata da tutta la documentazione pertinente al fine di consentire al titolare del trattamento, se necessario, di decidere in merito alla necessità di notificare tale violazione all'autorità di vigilanza competente. Dopo il consenso del titolare del trattamento, il responsabile del trattamento potrà notificare all'autorità di vigilanza competente (Garante Privacy), a nome e per conto del titolare del trattamento, le violazioni dei dati personali il più presto possibile e, comunque, non oltre 72 ore dopo esserne venuto a conoscenza, a meno che la violazione in questione non possa creare un rischio per i diritti e le libertà delle persone fisiche.

L'informazione al titolare del trattamento e la notifica contengono almeno:

- la descrizione della natura della violazione dei dati personali, comprese, ove possibile, le categorie e il numero approssimativo di persone interessate dalla violazione e le categorie e il numero approssimativo di record di dati interessati;
- il nome e i dettagli di contatto del responsabile della protezione dei dati o altro punto di contatto da cui possono essere ottenute informazioni aggiuntive;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o proposte dal titolare del trattamento per porre rimedio alla violazione dei dati personali, comprese, se del caso, misure per attenuare eventuali conseguenze negative.

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

12. assistere, nel contesto di conformità normativa, il titolare del trattamento. Se il responsabile del trattamento ritiene che un'istruzione costituisca una violazione del regolamento europeo sulla protezione dei dati o di qualsiasi altra disposizione del diritto dell'Unione o della legge sulla protezione dei dati degli Stati membri, egli deve segnalarlo al titolare del trattamento. Inoltre, se il responsabile del trattamento è tenuto a trasferire dati verso un paese terzo o verso un'organizzazione internazionale, fornirà specifiche garanzie a seguito di un quadro regolatorio riconosciuto tramite decisione di adeguatezza della Commissione Europea (come quella del 10 luglio 2023 che ha ufficialmente approvato il "EU-US Data Privacy Framework" ovvero il nuovo accordo sul trasferimento dei dati verso gli Stati Uniti) o, in assenza, idonee garanzie di natura contrattuale o pattizia (fra cui le norme vincolanti d'impresa "BCR" e le clausole contrattuali standard "SCC").

13. adeguare le misure di garanzia volte ad individuare idonee misure di sicurezza, ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento.

Il responsabile del trattamento si impegna ad attuare tutte le misure di garanzia volte ad individuare le misure di sicurezza, tecniche e organizzative, necessarie a garantire un livello di protezione adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Tra le misure di sicurezza valuta e documenta o meno l'adozione di:

- pseudonimizzazione e crittografia dei dati personali;
- sistemi per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- sistemi per ripristinare la disponibilità dei dati personali e accedervi in tempo utile in caso di incidente fisico o tecnico;
- sistemi per testare, analizzare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

Il responsabile del trattamento si impegna ad attuare ulteriori misure di sicurezza concordate anche successivamente alla stipula del presente contratto, eventualmente previste da linee guida, buone prassi, codici di condotta o meccanismi di certificazione qualora applicabili e rilevanti ai fini della protezione dei dati.

14. garantire il termine del trattamento dei dati. Al completamento dei servizi relativi al trattamento in oggetto, fatto salvo un ulteriore periodo di conservazione in relazione a contestazioni ed eventuali contenziosi derivanti dalla conclusione del rapporto professionale o in relazione a quanto imposto da norme di legge o da richiesta da parte dell'Autorità, il responsabile del trattamento si impegna, su esplicita richiesta del titolare, a:

- restituire tutti i dati personali al titolare del trattamento ovvero a restituire i dati personali ad altro responsabile del trattamento indicato dal titolare stesso;
- distruggere tutti i dati personali in suo possesso, successivamente al reso e dandone avviso al titolare del trattamento.

15. nominare un Responsabile della protezione dei dati, ove occorra. Il responsabile del trattamento informa il titolare del trattamento del nome e dei dettagli di contatto del suo responsabile della protezione dei dati, se ne ha designato uno conformemente all'art. 37 del regolamento europeo sulla protezione dei dati.

16. redigere il registro delle categorie di attività di trattamento eseguite per conto del titolare del trattamento ai sensi e conformemente all'art. 30 (comma 2) del GDPR. Il registro contiene, tra l'altro, il nome e gli estremi del titolare del trattamento a nome del quale agisce, eventuali sub-responsabili del trattamento ed eventualmente il responsabile della protezione dei dati.

17. fornire a richiesta del titolare del trattamento la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e consentire che il titolare del trattamento o altro revisore effettuino audit e verifiche, comprese le ispezioni. Inoltre, il responsabile del trattamento collabora, quando direttamente coinvolto, a questi audit e verifiche.

V. <u>Obblighi del titolare del trattamento nei confronti del responsabile del trattamento</u>

Il titolare del trattamento si impegna a:

1. fornire al responsabile del trattamento i dati di cui al punto II di queste clausole;
2. documentare per iscritto le istruzioni relative al trattamento dei dati da parte del responsabile del trattamento;
3. assicurare, in anticipo e per tutta la durata del trattamento, il rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati in capo al titolare relativamente al trattamento oggetto per presente accordo;
4. supervisionare il trattamento, compreso lo svolgimento di audit, verifiche e ispezioni presso il responsabile del trattamento.

Data 27-11-2023

Responsabile del trattamento
STUDIO LAROCCA STP S.R.L. UNIPERSONALE