



UMBERTO I

Azienda Pubblica di Servizi alla Persona

CONTRATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N. 679 (GDPR) E DELL'ART. 2 QUATERDECIES DEL D. LGS. 196/2003 E SS.MM. II.

TRA

ASP Umberto I (P. IVA 00226200939), in persona del suo Rappresentante legale *pro tempore*, con sede legale in Piazza della Motta, 12, Pordenone

(Titolare del trattamento/Titolare)

E

<!FORNITORE!> (P. IVA <!PIVAFORNITORE!>), in persona del suo legale rappresentante *pro tempore*, con sede/domiciliato in <!INDIRIZZOFORNITORE!>,

(Responsabile del trattamento/Responsabile)

premesse che:

- Il titolare del trattamento di dati personali può proporre una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo quale responsabile al trattamento dei dati che sia nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo di sicurezza;
- Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa richiesti dalle disposizioni *pro tempore* vigenti in materia e, altresì, garantisca la tutela dei diritti dell'interessato;
- Il responsabile deve procedere al trattamento secondo le istruzioni impartite dal titolare per iscritto, mediante il presente contratto e, o con eventuali accordi successivi;
- È intenzione del titolare consentire l'accesso sia al responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza è necessaria per adempiere ai compiti loro attribuiti;
- ASP Umberto I è titolare del trattamento di dati personali;
- <!FORNITORE!> svolge per <!RAGIONESOCIALE!> l'attività regolata dall'accordo in essere, sottoscritto in data <?DATAACCORDO?>;
- Sussistono in capo a <!FORNITORE!> i requisiti su detti, imposti dall'art.28 GDPR.

In virtù di quanto sopra premesso, che costituisce parte integrante del presente accordo, ASP Umberto I

nomina

<!FORNITORE!> "responsabile del trattamento"

ai sensi e agli effetti dell'art. 28 GDPR per i trattamenti di tutti i dati personali realizzati nell'ambito dell'incarico conferito.

In tale qualità <!FORNITORE!> è tenuto/a al rispetto delle disposizioni di Legge e di Regolamento in materia di tutela dei dati personali.

In particolare è tenuto a osservare le disposizioni che seguono:



UMBERTO I

Azienda Pubblica di Servizi alla Persona

1. DESCRIZIONE DEL TRATTAMENTO DEL RESPONSABILE

Il Responsabile è autorizzato a trattare, per conto del Titolare del trattamento, i dati personali necessari per fornire i servizi oggetto del contratto in essere tra le parti, che costituisce il presupposto necessario del presente.

2. OBBLIGHI DEL RESPONSABILE

2.1 Il Responsabile – per quanto di propria competenza – deve assistere e coadiuvare il Titolare nella corretta gestione delle operazioni di trattamento che dovranno essere effettuate nel pieno rispetto degli obblighi previsti dal GDPR. A tale proposito, il Responsabile deve trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento. Qualora ricorra quest'ultima ipotesi, salvo che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico, il Responsabile deve informare il Titolare circa tale obbligo giuridico prima del trattamento.

2.2 Il Responsabile assicura per sé stesso e per le persone espressamente autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate. Sarà cura del Responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Titolare, in relazione alle operazioni di Trattamento eseguite.

2.3 Il Responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e, più in generale, di ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché dei provvedimenti dell'Autorità Garante competente e delle linee guida adottate dall'European Data Protection Board.

2.4 Il Responsabile, altresì, trattandosi di Suoi strumenti, prodotti, applicazioni o servizi, applicherà i principi della Privacy by design e della Privacy by default.

2.5 Il Responsabile garantisce di attuare misure tecniche e organizzative adeguate al fine di assicurare un livello di sicurezza congruo al rischio in merito al trattamento dei dati effettuato (ai sensi dell'allegato A).

2.6 Il Responsabile del trattamento deve riferire, su richiesta del Titolare, i dettagli relativi all'adempimento di quanto disposto dal presente atto nonché dalla normativa privacy vigente, attraverso relazioni scritte ovvero compilazione di check list che verranno fornite all'uopo.

2.7 Inoltre, il Responsabile deve contribuire alle attività di revisione, comprese le ispezioni, e ad informare prontamente il Titolare del trattamento di ogni questione rilevante ai fini del presente atto, quali a titolo indicativo:

- Istanze di interessati;
- Richieste del Garante;
- Esiti delle ispezioni;
- Violazioni del GDPR o di altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, o la messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali (ai sensi dell'allegato A).

2.8 Qualora il Responsabile si avvalga di persone appositamente autorizzate al trattamento dei dati, che operano sotto la sua responsabilità in quanto deputati alle operazioni di Trattamento, è tenuto a fornire loro specifiche istruzioni scritte



UMBERTO I

Azienda Pubblica di Servizi alla Persona

ed a vigilare sul loro operato, fatte salve specifiche disposizioni di legge.

2.9 Ove applicabile, il Responsabile deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del Titolare del trattamento (art. 30 GDPR).

Il Responsabile del trattamento deve mettere il Registro a disposizione dell'Autorità di controllo, se richiesto, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati (Considerando 82 GDPR).

2.10 Nel caso in cui gli interessati esercitino presso il Responsabile delle domande di esercizio dei loro diritti, lo stesso dovrà trasmetterle, entro cinque giorni lavorativi, al Titolare del Trattamento, fornendo altresì una relazione dettagliata dei termini e modalità del trattamento posto in essere in ragione di questo accordo e comunque collaborando con il Titolare per fornire all'interessato le informazioni e i chiarimenti richiesti.

2.11 Il Responsabile del trattamento è tenuto altresì a:

- cooperare con l'Autorità di Controllo quando richiesto;
- supportare l'attività svolta dal DPO (Data Protection Officer - Responsabile della Protezione dei Dati) per conto del Titolare del trattamento (artt. 37, 38 GDPR).

3. NOMINA DI ULTERIORE RESPONSABILE DEL TRATTAMENTO (O SUB RESPONSABILE)

3.1 Il titolare del trattamento deve autorizzare per iscritto a sub-delegare ad altro Responsabile trattamenti di dati demandati in forza del contratto tra le parti.

A tale autorizzazione segue l'atto di nomina del sub-responsabile che deve essere inoltrato dal Responsabile al Titolare.

3.2 Parimenti, il Responsabile informa il Titolare anche di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili, così da permettergli di esercitare il diritto di opporsi.

3.3 Spetta in capo al Responsabile del trattamento l'obbligo di assicurarsi che il sub-responsabile presenti le garanzie sufficienti per quanto riguarda l'adozione delle misure tecniche e organizzative necessarie affinché il trattamento dei dati sia conforme alle esigenze del GDPR. Se il sub-responsabile non rispetta gli obblighi in materia di protezione dei dati personali, il Responsabile risponde solidalmente nei confronti del Titolare del trattamento.

4. VERIFICHE PERIODICHE/ AUDIT

4.1 Il Responsabile deve fornire la massima disponibilità e collaborazione, consentendo, se necessario, l'accesso ai locali, nonché la verifica delle procedure applicate nella gestione dei documenti cartacei ed elettronici affinché il Titolare possa svolgere, anche tramite consulenti ed addetti di propria fiducia, le "verifiche periodiche", previste dall'art.28 GDPR, necessarie per verificare il rispetto degli obblighi di questo accordo e della normativa sopra citata.

4.2 Ogni qualvolta il Titolare ne faccia richiesta, il Responsabile riferisce per iscritto i dettagli relativi all'adempimento di quanto disposto dalla Legge e dal presente atto di nomina.

5. GESTIONE MODULISTICA PRIVACY

5.1 Il Responsabile deve operare in maniera conforme ai principi di efficienza e trasparenza, tramite adeguate procedure e garantendo la custodia, la non alterazione e l'agevole reperimento della documentazione relativa agli adempimenti formali prescritti dalla normativa.

5.2 Il Responsabile, su richiesta del Titolare, deve coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi al Garante per la protezione dei dati personali o all'Autorità giudiziaria ordinaria anche consentendogli la tempestiva esibizione della modulistica privacy e dei documenti probatori rientranti nella competenza del Responsabile stesso.



UMBERTO I

Azienda Pubblica di Servizi alla Persona

6. CESSAZIONE DEL RAPPORTO

All'atto della cessazione, per qualsiasi causa, delle operazioni di trattamento da parte del Responsabile, quest'ultimo restituisce tempestivamente al Titolare, salvo comprovati obblighi di legge, e comunque entro un mese dalla cessazione, i dati personali oggetto delle operazioni di trattamento, su qualunque supporto detenuto (cartaceo o informatico, originali e copie), rilasciando contestualmente un'attestazione scritta che presso la propria struttura non ne esista alcuna ulteriore copia.

7. DURATA

7.1 Il presente atto ha la durata del rapporto tra le parti, salvo cessazione per qualsiasi motivo intervenuta.

7.2 Lo stesso sarà rinnovato di diritto in caso di rinnovo dell'accordo principale.

8. REVOCA

Il Titolare ha facoltà di revocare il presente mandato, nel caso di reiterate violazioni del GDPR da parte del Responsabile, con effetto immediato, previa notifica scritta allo stesso via PEC e senza che nulla gli sia ulteriormente dovuto.

9. LEGGE APPLICABILE E FORO COMPETENTE

Il presente contratto è disciplinato secondo la Legge Italiana. Per quanto ivi non esplicitamente previsto si applicheranno le norme del Codice Civile nonché le altre norme giuridiche inderogabili aventi efficacia di legge.

Tutte le controversie derivanti dal presente contratto, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, saranno di competenza esclusiva del Foro già individuato nell'accordo principale.

<!LUOGO!>, <?DATA?>

ASP Umberto I

Firma

<!FORNITORE!>

Firma



UMBERTO I

Azienda Pubblica di Servizi alla Persona

ALLEGATO A

MISURE DI SICUREZZA

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, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il Responsabile del trattamento, se necessario e su richiesta, dovrà altresì assistere il Titolare del trattamento nella redazione del "DPIA" (Data Protection Impact Assessment), contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere in merito un parere al DPO (Data Protection Officer) (art.35 e C.90 GDPR).

VIOLAZIONE DEI DATI

Se dovesse venire a conoscenza di una violazione dei dati personali (Data Breach), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).

E' opportuno che il Responsabile del trattamento si doti di una opportuna policy che specifichi le procedure che consentono di individuare prontamente le violazioni dei dati subite (Data Breach) e le relative risposte.

Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

Nello specifico dovranno essere documentati:

- a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo



UMBERTO I

Azienda Pubblica di Servizi alla Persona

di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

- b) il nome e i dati di contatto de DPO (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
- c) la descrizione delle probabili conseguenze della violazione dei dati personali;
- d) le descrizioni delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (Data breach) prevista dall'art. 33 comma 3 del GDPR.