

**CONTRATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO
E CONFERIMENTO DELLE RELATIVE ISTRUZIONI**

(Riferimento Codice fascicolo N° 17.2-2018-104)

Tra

TRENTINO DIGITALE S.P.A. con sede legale in Trento (38121), Via G. Gilli n. 2, Capitale Sociale €6.433.680,00 interamente versato, Codice Fiscale, Partita I.V.A e iscrizione al Registro delle Imprese di Trento al n. 00990320228, Società soggetta ad attività di direzione e coordinamento della Provincia Autonoma di Trento,

nella persona del dott. xxx, Legale Rappresentante della Società, che ha delegato il Responsabile pro tempore della Direzione XXXX Dott. YYYY al trattamento dei dati ed al compimento delle azioni ad esso afferenti (di seguito "Trentino Digitale" o "Titolare");

e

XXX, xxx, con sede in xxx (xxx), via xxx, Codice Fiscale e Partita IVA xxx, in persona del legale rappresentante/procuratore Sign.Dott.xxx (nel seguito "xxx" o "Responsabile");

Congiuntamente "le Parti".

Premesso che:

- tra Trentino Digitale e la/ilXXX.....intercorre un rapporto negoziale, in forza del/della contratto/convenzione sottoscritto/a tra le Parti in dataprotocollo Trentino Digitale n°..... avente oggetto:.....;

- tale rapporto contrattuale implica, necessariamente, il trattamento, da parte della/del ...XXX, di dati personali di cui Trentino Digitale è Titolare del trattamento;

- il 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)» (di seguito "GDPR" o "Regolamento"), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, prevede la figura del Responsabile del trattamento (artt. 28-29);

- ai sensi dell'art. 28, paragrafo 1, del Regolamento, "Qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato";

- a seguito delle garanzie offerte e delle dichiarazioni rilasciate dalla/dal XXX, in forza di quanto previsto al considerando n. 81 del Regolamento, tale soggetto è stato ritenuto idoneo ad assumere la qualifica di Responsabile del trattamento;

Tutto ciò premesso e considerato,

che costituisce parte integrante e sostanziale del presente atto,

si conviene quanto segue.

Art. 1

OGGETTO

Ai sensi e per gli effetti dell'art. 28 del Regolamento, con il presente contratto (di seguito, il "Contratto") Trentino Digitale, in qualità di "Titolare del trattamento" (di seguito, il "Titolare"), nomina XXX Responsabile del trattamento" (di seguito, il "Responsabile").

Il Responsabile, pertanto, si impegna al rigoroso rispetto delle prescrizioni del presente contratto con la diligenza di cui all'art. 1176, comma 2, del Codice Civile della predetta normativa comunitaria, della relativa disciplina nazionale, nonché delle prescrizioni dell'Autorità di controllo.

Art. 2

AMBITO E LIMITI DEL TRATTAMENTO

Il Responsabile è autorizzato a trattare, per conto del Titolare, i dati personali necessari a fornire il servizio o i servizi ad esso affidati attraverso il contratto citato al primo punto delle premesse.

Il dettaglio delle attività, della natura, delle finalità, della tipologia di dati personali conferiti, nonché di altre informazioni rilevanti a descrivere il trattamento che sarà effettuato da parte del Responsabile, è descritto nell'**Allegato A** del presente accordo.

Il Responsabile si impegna a trattare i dati personali soltanto su istruzione documentata del Titolare; in particolare, in relazione al rapporto contrattuale di cui al primo punto delle premesse, il Responsabile potrà trattare i dati, con o senza strumenti automatizzati, esclusivamente per le finalità espresse e compiendo le operazioni esplicitamente autorizzate dal Titolare, come descritte nell'**Allegato A**.

Il Responsabile informerà immediatamente il Titolare qualora, a suo parere, un'istruzione violasse il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Qualora la normativa, comunitaria o nazionale, imponesse al Responsabile il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, lo stesso Responsabile informerà il Titolare di tale obbligo giuridico prima del relativo trasferimento, salvo che la normativa in questione vieti tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile è consapevole ed accetta che i propri dati personali possano essere pubblicati sul sito istituzionale o sulla bacheca del Titolare per finalità di trasparenza nei confronti degli interessati.

Art. 3

OBBLIGHI DEL RESPONSABILE

In ogni fase e per ogni operazione del trattamento, il Responsabile dovrà garantire il rispetto dei principi comunitari di cui agli artt. 5 e 25 del Regolamento, e nazionali in ambito di protezione dei dati personali.

Inoltre il Responsabile dovrà in particolare:

- a) garantire che i propri addetti che trattano dati personali siano stati specificamente autorizzati, adeguatamente istruiti e si siano impegnati alla riservatezza, o abbiano un adeguato obbligo legale di riservatezza;
- b) adottare tutte le misure di sicurezza organizzative e tecniche richieste ai sensi dell'articolo 32 del Regolamento, se non diversamente specificate dall'**Allegato B** del presente contratto.
- c) assistere il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (Capo III del Regolamento), nonché informare tempestivamente il Titolare dei reclami eventualmente presentati dagli interessati;
- d) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Contratto, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare, dal suo Data Protection Officer, o da un altro soggetto a ciò deputato;
- e) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento.

In particolare, relativamente alla predisposizione della valutazione di impatto” (“Data privacy impact assessment”, di cui agli artt. 35 e 36 del Regolamento), nel caso in cui il Responsabile fornisca al Titolare gli strumenti/applicativi informatici e/o gestisca gli stessi strumenti/applicativi informatici del Titolare, lo stesso sarà tenuto a predisporre ed aggiornare l’analisi dei rischi (probabilità di violazione della sicurezza) degli strumenti/applicativi informatici, comunicandola al Titolare, adottando i criteri di valutazione forniti da quest’ultimo.

Con riferimento ai casi di cui agli artt. 33 e 34 del Regolamento, il Responsabile si obbliga a segnalare al Titolare e/o al Data Protection Officer di quest’ultimo, qualsiasi episodio di “data breach”, non appena venutone a conoscenza, senza alcun ritardo entro e non oltre 12 ore. Inoltre, si impegna a fornire al Titolare tutti gli elementi, le informazioni, ai sensi dell’art. 33 del Regolamento, e l’assistenza necessaria alla comprensione dell’evento e all’eventuale compilazione della notifica all’Autorità di Controllo ed eventualmente agli interessati.

In particolare, la comunicazione al Titolare della avvenuta violazione ai dati dovrà corrispondere almeno ai seguenti punti:

- Natura della violazione dei dati personali;
- Categoria degli interessati;
- Data e orario in cui si è verificato l’incidente;
- Interventi attuati o che si prevede di attuare per porre rimedio alla violazione o limitarne gli effetti negativi;
- Comunicazione avvio assessment per individuare il numero approssimativo di interessati i cui dati personali sono stato oggetto dell’incidente
- Indicazione dei referenti interni che stanno gestendo la violazione.

f) provvedere alla nomina del Data Protection Officer (di seguito, "DPO") nei casi prescritti dall'art. 37 del Regolamento, garantendo il rispetto delle prescrizioni di cui all'art. 38, anche allo scopo di consentire al medesimo DPO l'effettivo adempimento dei compiti di cui art. 39 del Regolamento;

g) qualora sia necessario fornire accessi di amministratori alle proprie risorse, il Responsabile deve provvedere alla designazione per iscritto del/degli Amministratore/i di Sistema secondo i criteri di individuazione e selezione previste dall'Autorità di controllo con provvedimento dd. 27/11/2008 e s.m.i., conservando l'elenco degli stessi Amministratori, verificandone annualmente l'operato ed adottando sistemi idonei alla registrazione dei relativi accessi logici (da conservare con caratteristiche di inalterabilità e integrità per almeno per 6 mesi).

Qualora l'attività degli stessi Amministratori di Sistema riguardasse, anche indirettamente, servizi o sistemi che trattano, o che permettono il trattamento, di informazioni di carattere personale dei dipendenti del Titolare, comunicare a quest'ultimo l'identità degli Amministratori di Sistema (provvedendo a dare idonea informativa, ex art. 13 del Regolamento, agli stessi Amministratori);

h) provvedere alla predisposizione del Registro delle attività del trattamento nei termini di cui all'art. 30 del Regolamento, mettendolo tempestivamente a disposizione del Titolare, o dell'Autorità di controllo, in caso di relativa richiesta;

i) comunicare al Titolare i nominativi di riferimento per l'esecuzione del Contratto, nonché il nominativo dell'eventuale DPO;

j) il Responsabile non potrà trasferire verso Paesi terzi (non appartenenti all'UE o allo Spazio Economico Europeo) ovvero organizzazioni internazionali i dati personali oggetto del trattamento senza previa autorizzazione scritta, specifica o generale, del Titolare; qualora i dati personali fossero trasferiti verso Paesi terzi ovvero organizzazioni internazionali, il Responsabile dovrà garantire il rispetto delle condizioni di cui agli art. 44 e ss. del Capo V del Regolamento;

k) alla scadenza del rapporto contrattuale di cui in premessa (ivi compresi i casi di risoluzione o recesso), o al più tardi al termine dell'esecuzione delle relative attività/prestazioni e, quindi, delle conseguenti operazioni di trattamento, fatta salva una diversa determinazione del Titolare indicata in allegato A al punto 6, dovrà provvedere alla cancellazione (ivi compresa ogni eventuale copia esistente) dei dati personali in oggetto (dandone conferma scritta al Titolare), a meno che la normativa comunitaria o nazionale ne preveda la conservazione ed esclusa ogni altra forma di conservazione anche per finalità compatibili.

l) in caso di trattamento con modalità automatizzate il Responsabile garantisce che, prima di effettuare la cancellazione predetta, su richiesta del Titolare e senza costi aggiuntivi, potrà effettuare la trasmissione sicura dei dati personali ad altro soggetto, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, beninteso qualora il destinatario sia attrezzato a riceverli. La mancata trasmissione dei dati personali nei termini sopra indicati o la mancata trasmissione dei dati personali nel formato sopra indicato costituisce grave inadempimento contrattuale.

Art. 4

SUB-RESPONSABILE

Il Responsabile potrà ricorrere ad altro ulteriore Responsabile del trattamento (di seguito il sub-Responsabile). Il Responsabile informerà il Titolare prima della nomina e di eventuali modifiche riguardanti l'aggiunta o la sostituzione di ulteriori sub-Responsabili, dando così al Titolare l'opportunità di opporsi per giustificati motivi.

In ogni caso, qualora il Responsabile ricorresse ad un sub-Responsabile per l'esecuzione di specifiche attività di trattamento per conto del Titolare, dovrà sottoscrivere, con tale sub-Responsabile, un contratto (o altro atto giuridico) analogo al presente Contratto stipulato in forma scritta, anche in formato elettronico imponendo al sub-responsabile gli stessi obblighi in materia di protezione dei dati contenuti nel presente Contratto (e in ogni altro atto giuridico o addendum intervenuto tra le Parti) e prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento, nonché della relativa disciplina nazionale.

Resta inteso che, laddove il sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile sarà ritenuto integralmente responsabile nei confronti del Titolare dell'adempimento degli obblighi del sub-Responsabile.

Art. 5

RESPONSABILITA'

Ferma ogni ulteriore responsabilità nei confronti del Titolare, ai sensi dell'art. 82, paragrafo 2, del Regolamento il Responsabile del trattamento risponde direttamente per il danno causato dal trattamento se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme, o contrario, rispetto alle istruzioni impartite dal Titolare del trattamento.

In caso di azione di risarcimento civile, o responsabilità amministrativa, promossa nei confronti del Titolare per i danni provocati, o le violazioni commesse dal Responsabile a seguito di inadempienze normative o contrattuali, il Responsabile stesso manleva integralmente il Titolare, ogni eccezione rimossa. Analogamente, il Responsabile manleva integralmente il Titolare, ogni eccezione rimossa, in caso di applicazione di sanzioni da parte dell'Autorità di controllo per inadempienze normative o contrattuali commesse dallo stesso Responsabile.

Art. 6

DURATA

Il presente Contratto ha la medesima durata del contratto principale richiamato in premessa ivi comprese proroghe ed estensioni dello stesso; la risoluzione o il recesso dello stesso produrrà medesimo effetto sul presente Contratto.

Art. 7

FORO COMPETENTE

Per ogni controversia riguardante il presente Contratto è competente il Foro di Trento.

ALLEGATI PARTE INTEGRANTE:

A - Istruzioni relative al trattamento dei dati

B – Misure di sicurezza

PER XXX	PER TRENTINO DIGITALE
Il Legale Rappresentante/Procuratore	Il Legale Rappresentante /Dirigente Delegato
- xxx-	xxxxxxx
<i>(Documento firmato digitalmente)</i>	<i>(Documento firmato digitalmente)</i>

Il Responsabile, ai sensi e per gli effetti dell'art. 1341 c.c., accetta e sottoscrive espressamente le seguenti clausole:

Art. 1 – Oggetto

Art. 2 – Ambito e limiti del trattamento

Art. 3 - Obblighi del responsabile

Art. 4 – Sub-responsabile

Art. 5 – Responsabilità

Art. 7 – Foro competente

PER XXX	PER TRENTINO DIGITALE
Il Legale Rappresentante/Procuratore	Il Legale Rappresentante /Dirigente Delegato
- xxx-	xxxxxxxxx
<i>(Documento firmato digitalmente)</i>	<i>(Documento firmato digitalmente)</i>

ALLEGATO A

ISTRUZIONI RELATIVE AL TRATTAMENTO DEI DATI

ALLEGATO A1 – Servizio Help Desk Base

ISTRUZIONI RELATIVE AL TRATTAMENTO DEI DATI

1. Categorie di dati personali:

I dati trattati appartengono alla categoria dei dati “comuni” e si riferiscono a nome e cognome, telefono, email, codice fiscale, data di nascita, luogo di lavoro.

2. Indicazione delle Categorie di interessati ai quali si riferiscono i Dati Personali:

La categoria di interessati è costituita da clienti, fornitori e utenti.

3. Indicazione delle finalità del trattamento

I dati personali dovranno essere trattati esclusivamente ai fini dell’esecuzione dell’incarico affidato, e di seguito elencati:

- registrazione e gestione delle richieste/segnalazioni ricevute

4. Indicazione delle attività di trattamento svolte dal Responsabile

- Operazioni di trattamento Generali: Raccolta, Registrazione, Modifica, Estrazione e Consultazione
- Operazioni di trattamento Particolari ¹ : Non sono previste operazioni di trattamento Particolari

5. Destinatari dei dati personali

N.A.

6. Indicare come deve avvenire la restituzione al termine del contratto.

Al termine del contratto non sussistono casistiche per le quali il Responsabile deve restituire dati personali al Titolare.

7. Varie ed eventuali a seconda dei casi.

N.A.

¹ LEGENDA:

Comunicazione=Trasferimento di dati a terzi, dove terzi sono soggetti ben identificati differenti dal Titolare, dai Responsabili, dall’Interessato e dagli altri Autorizzati al trattamento;

Diffusione=Dare conoscenza dei dati a soggetti indeterminati (es. pubblicazione web);

Interconnessione=Utilizzo di più banche dati con strumenti elettronici (es. auth federata, tibco, vaccinazione/studenti, generalmente i webservice) che contengono dati la cui titolarità non è del titolare.

Limitazione=Consiste nel blocco del trattamento dei dati su istanza dell’interessato al verificarsi di determinate circostanze; in caso di esercizio di tale diritto ogni trattamento, tranne la conservazione, è vietato.

Cancellazione=Eliminazione di dati tramite utilizzo di strumenti elettronici (esistono altre copie tipo backup). Esempio cancellazione di intero dataset oppure in caso di particolari richieste, l’oscuramento del singolo record del db in linea al fine di mantenere l’integrità del database (es. asterischi al posto dei dati).

Distruzione=Eliminazione di dati tramite utilizzo di strumenti elettronici anche nei backup. Esempio cancellazione di intero dataset, e di tutte le sue copie, oppure in caso di particolari richieste, l’oscuramento del singolo record del db in linea al fine di mantenere l’integrità del database (es. asterischi al posto dei dati). In questo caso, bisogna documentare l’impossibilità di distruggere i singoli record conservati nei backup storici senza compromettere gli stessi backup.

ALLEGATO A2 - < Nome Servizio>**ISTRUZIONI RELATIVE AL TRATTAMENTO DEI DATI****1. Categorie di dati personali**

[dettagliare e descrivere quali sono le tipologie (Comune, Particolare, Giudiziario) e la descrizione dei Dati Personali oggetto del trattamento]

2. Indicazione delle Categorie di interessati ai quali si riferiscono i Dati Personali

[dettagliare e descrivere le categorie di Interessati per es. dipendenti, clienti, fornitori, candidati, cittadini, utenti]

3. Indicazione delle finalità del trattamento

I dati personali dovranno essere trattati esclusivamente ai fini dell'esecuzione dell'incarico affidato, e di seguito elencati: *dettagliare e descrivere le finalità del trattamento ES. gestione database xxxxyyyy...*

4. Indicazione delle attività di trattamento svolte dal Responsabile

- Operazioni di trattamento Generali: ..., ...,... *[indicare quali sono le operazioni di trattamento tra le seguenti: Raccolta, Registrazione, Organizzazione, Conservazione, Modifica, Estrazione e Consultazione].*
- Operazioni di trattamento Particolari ² :

[indicare quali sono le operazioni di trattamento tra le seguenti: Comunicazione, Diffusione, Interconnessione, Limitazione, Cancellazione, Distruzione secondo lo schema di seguito riportato:]

(compilare di seguito solo quelle previste)

² LEGENDA:

Comunicazione=Trasferimento di dati a terzi, dove terzi sono soggetti ben identificati differenti dal Titolare, dai Responsabili, dall'Interessato e dagli altri Autorizzati al trattamento;

Diffusione=Dare conoscenza dei dati a soggetti indeterminati (es. pubblicazione web);

Interconnessione=Utilizzo di più banche dati con strumenti elettronici (es. auth federata, tibco, vaccinazione/studenti, generalmente i webservice) che contengono dati la cui titolarità non è del titolare.

Limitazione=Consiste nel blocco del trattamento dei dati su istanza dell'interessato al verificarsi di determinate circostanze; in caso di esercizio di tale diritto ogni trattamento, tranne la conservazione, è vietato.

Cancellazione=Eliminazione di dati tramite utilizzo di strumenti elettronici (esistono altre copie tipo backup). Esempio cancellazione di intero dataset oppure in caso di particolari richieste, l'oscuramento del singolo record del db in linea al fine di mantenere l'integrità del database (es. asterischi al posto dei dati).

Distruzione=Eliminazione di dati tramite utilizzo di strumenti elettronici anche nei backup. Esempio cancellazione di intero dataset, e di tutte le sue copie, oppure in caso di particolari richieste, l'oscuramento del singolo record del db in linea al fine di mantenere l'integrità del database (es. asterischi al posto dei dati). In questo caso, bisogna documentare l'impossibilità di distruggere i singoli record conservati nei backup storici senza compromettere gli stessi backup.

- *Comunicazione*
 - A CHI:
 - COSA:
 - QUANDO:
- *Diffusione*
 - A CHI:
 - COSA:
 - QUANDO:
- *Interconnessione*
 - DA DOVE:
 - COSA:
 - QUANDO:
- *Limitazione*
 - A CHI:
 - COSA:
 - QUANDO:
- *Cancellazione*
 - COSA:
 - QUANDO:
- *Distruzione*
 - COSA:
 - QUANDO:

5. Destinatari dei dati personali

[Indicare i destinatari dei dati personali qualora i dati stessi siano o saranno trasmessi/comunicati ad uno o più soggetti determinati e/o qualora i dati vengano gestiti esternamente da una terza parte con cui il Responsabile ha un obbligo o un contratto per eseguire delle operazioni di trattamento dati (es. enti pubblici, fornitori terzi). in quest'ultimo caso il Responsabile provvederà alla Nomina di un Sub-Responsabile del Trattamento.]

6. Indicare come deve avvenire la restituzione al termine del contratto.

7. Varie ed eventuali a seconda dei casi.

ALLEGATO B

MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE

ALLEGATO B1 – Servizio Help Desk Base

MISURE DI SICUREZZA ORGANIZZATIVE

Responsabile avrà cura che l'accesso ai dati personali, memorizzati sui sistemi messi a disposizione da parte del Titolare,

- avvenga nel rispetto delle misure di sicurezza garantite dalle credenziali di accesso, fornite dal Titolare su richiesta del Responsabile a titolo di credenziali personali per ciascun operatore.
- avvenga solo da parte di personale autorizzato e con le sole finalità di trattamento consentite dal Titolare.

Sarà cura del Responsabile comunicare al Titolare l'eventuale cessazione del rapporto di lavoro di un operatore o la cessazione del diritto dell'operatore ad accedere ai sopra citati sistemi del Titolare.

MISURE DI SICUREZZA TECNICHE

Tutte le stazioni di lavoro (contrattualmente acquisite autonomamente dal Responsabile) dovranno essere protette da username e password.

In relazione alla definizione e gestione delle password dovranno essere adottate misure di sicurezza adeguate, quali ad esempio il rispetto di requisiti adeguati di complessità e l'utilizzo e conservazione in forma riservata.

ALLEGATO B2 - < Nome Servizio >**MISURE DI SICUREZZA TECNICO-ORGANIZZATIVE****CASO 1**

Ci si attiene a quanto previsto dall'art. 3 lettera b) del presente contratto, con rimando all'art.32 del GDPR, senza ulteriore specificazione di misure tecnico-organizzative.

CASO 2

Devono essere rispettate le misure tecnico-organizzative di seguito elencate:

- a) Già previste nel bando di gara, ordine di acquisto, contratto di affidamento;
- b) Specificatamente elencate nel presente allegato definendo le Modalità del Trattamento le Misure organizzative e le Misure tecniche