



ACCORDO PER LA NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

La Città Metropolitana di Catania, in persona del legale rappresentante pro tempore, con sede in Catania, Via Prefettura, 14 – 95124 (CT), C.F./P. IVA: 00397470873, in qualità di Titolare del trattamento ai sensi del Regolamento (UE) 2016/679 (di seguito “Titolare”)

e

[**ragione sociale**], in persona del legale rappresentante pro tempore, con sede in [redacted], Via [redacted], p. iva [redacted] (di seguito: “Terzo” o “Responsabile del Trattamento”),

Premesso che

- l'art. 4, paragrafo 1, numero 8, del Regolamento (UE) 2016/679 definisce il “*Responsabile del trattamento*” come la persona fisica o giuridica, l'autorità pubblica, il servizio o organismo che tratta dati personali per conto del titolare del trattamento;
- l'art 28 del predetto Regolamento dispone che:

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, 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 presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati



personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti 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; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento.



Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

- L'art. 29 del medesimo Regolamento prevede che:

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

- Il Titolare del trattamento in relazione ai Dati Personali trattati, determina le finalità ed i mezzi del trattamento;

in data **xx/xx/xx** il Titolare ha sottoscritto con **[ragione sociale]** il contratto avente oggetto

- con il presente atto - che costituisce parte integrante e sostanziale del contratto di cui sopra - , il Titolare del trattamento, intende nominare **[ragione sociale]**, in persona del legale rappresentante pro tempore, che accetta, Responsabile del trattamento, ai sensi di quanto disposto dall'art. 28 del GDPR;



- con la sottoscrizione del presente documento il Titolare e il Responsabile del Trattamento intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali effettuato dal Responsabile del trattamento per conto del Titolare ai sensi dell'art. 28, paragrafo 3 del Regolamento.

Tanto premesso e considerato, le Parti, come sopra identificate, convengono e stipulano quanto segue:

Definizioni:

Fatta eccezione per i termini e le espressioni altrimenti definiti nel presente Accordo, i termini e le espressioni contrassegnate da iniziali maiuscole avranno il significato di seguito specificato:

“GDPR”	indica 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).
“Autorità di Controllo”	indica il Garante per la protezione dei 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.
“Accordo di trasferimento dei dati”	indica ogni accordo stipulato tra le parti e finalizzato al trasferimento legittimo dei Dati Personali.
“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.
“Codice”	il D.Lgs. n. 196/2003 “Codice in materia dei dati personali” così come successivamente integrato e modificato (da ultimo del D.Lgs. n. 101/2018).
“Comitato Europeo per la protezione dei dati”	indica l'organismo dell'Unione Europea dotato di personalità giuridica istituito ai sensi degli artt. 68 e ss. del GDPR.



“Comunicazione”	dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, del responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'art. 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.
“Contratto”	indica l'accordo in essere tra le Parti.
“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.
“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.
“Diffusione”	Indica il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
“Gruppo di Lavoro Articolo 29”	indica il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE.
“Interessato”	la persona fisica identificata o identificabile cui si riferiscono i Dati Personali.
“Responsabile del trattamento”	Indica chi effettua un trattamento dati per conto del titolare del trattamento.
“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.

“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.

“Trattamento”

Indica 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.

1. Nomina del Responsabile del trattamento

Con la sottoscrizione del presente atto, che forma parte integrante del Contratto, il Titolare nomina **[ragione sociale]** quale Responsabile del Trattamento ai sensi dell'art. 28 del GDPR, con l'incarico di effettuare le operazioni di trattamento sui Dati Personali, di cui entra in possesso o ai quali ha comunque accesso, necessarie all'adempimento degli obblighi derivanti dal Contratto e di eventuali servizi accessori allo stesso.

Il Responsabile del Trattamento, con la sottoscrizione del presente accordo, accetta tutti i termini sottoindicati, conferma la diretta e approfondita conoscenza degli obblighi che si assume e si impegna a procedere al trattamento dei Dati Personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina o a quelle ulteriori che saranno conferite nel corso delle attività prestate in suo favore.

Il Responsabile del Trattamento prende atto che l'incarico di effettuare le operazioni di trattamento sui Dati Personali quale Responsabile del trattamento è affidato per l'esclusiva ragione che il profilo societario, in termini di proprietà, risorse umane, organizzative ed attrezzature, è stato ritenuto idoneo a soddisfare i requisiti di esperienza, capacità, affidabilità previsti dalla vigente normativa. Qualsiasi mutamento di tali requisiti, che possa sollevare incertezze sul loro mantenimento, dovrà essere preventivamente segnalato al



Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di recesso, senza penali ed eccezioni di sorta.

2. Garanzie

Il Responsabile del trattamento conferma di possedere le garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli Interessati.

Il Responsabile si impegna pertanto ad operare secondo il principio di responsabilizzazione, fin dall'inizio del trattamento e per progettazione predefinita, per ridurre al minimo i rischi connessi al trattamento e per garantire il pieno rispetto delle disposizioni vigenti in materia di trattamento dei dati personali.

3. Finalità, categorie di dati trattati, categorie di interessati.

Il trattamento deve essere svolto da parte del Responsabile del trattamento in esecuzione del vigente rapporto contrattuale con il Titolare e per le finalità ad esso relative, nonché per il tempo strettamente necessario al perseguimento di tali finalità.

In particolare, le categorie di dati che saranno trattati e le tipologie di trattamento che sarà eseguito dal Responsabile del trattamento sono di seguito indicate:

Categoria di dati Trattati	Finalità del Trattamento	Categoria di interessati
[ad es. dati personali di identificazione, dati di identificazione elettronica, di identificazione finanziaria, dati di stato civile, dati sulla condizione lavorativa, curriculum, presenze, medicina del lavoro] oppure [dati particolari: genetici, biometrici, sulla salute, giudiziari, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, vita o orientamento sessuale, condanne penali, dati protetti dal segreto professionale, dati di geolocalizzazione]	[indicare la finalità del servizio/oggetto del contratto]	[ad es. Utenti/cittadini, dipendenti, consulenti/professionisti, fornitori/clienti, Amministratori/membri di organismi di controllo, Revisori, iscritti ad albi o elenchi...]

Resta inteso che il trattamento di categorie particolari di dati e di dati penali sarà autorizzato nei soli limiti di esenzione dal divieto generale di cui all'art. 9 e 10 GDPR, secondo le misure



stabilite ivi nonché nel Codice agli artt. 2-ter e seguenti, ivi comprese le regole deontologiche e le misure di garanzia che saranno volta per volta emesse.

4. Diritti del Titolare

Il Titolare ha diritto di ottenere dal Responsabile del trattamento tutte le informazioni relative alle misure organizzative e di sicurezza da questo adottate necessarie per dimostrare il rispetto delle istruzioni e degli obblighi affidati.

Lo stesso Titolare, inoltre, ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di audit in ambito protezione dei dati personali e sicurezza, avvalendosi anche di personale espressamente incaricato a tale scopo, tenuto al segreto sulle informazioni così acquisite e/o elaborate, presso le sedi del Responsabile del trattamento, come indicato al punto 11.

5. Obblighi del Responsabile

Nell'adempimento delle proprie obbligazioni il Responsabile, i suoi dipendenti ed ogni eventuale Sub-responsabile previamente autorizzato dal Titolare, che effettuino il Trattamento di Dati Personali del Titolare, si obbligano a rispettare il GDPR ed ogni altra istruzione impartita dal Titolare, nonché a tener conto dei provvedimenti tempo per tempo emanati dall'Autorità di Controllo italiana, dal Gruppo di Lavoro Articolo 29 e dal Comitato Europeo per la protezione dei dati, inerenti al trattamento svolto.

Il Responsabile è tenuto a svolgere, con correttezza e buona fede, le seguenti attività:

- a) rispettare i principi di liceità, correttezza, trasparenza, pertinenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione, tutela fin dall'inizio del trattamento e per progettazione definita, di cui al GDPR;
- b) mantenere e far mantenere ai propri incaricati la massima riservatezza sui dati trattati;
- c) eseguire operazioni di trattamento sui dati al solo scopo di eseguire le prestazioni oggetto del Rapporto e di adempiere ad altre previsioni normative, evitando qualsiasi ulteriore operazione che non sia strettamente necessaria a tale esecuzione;
- d) rispettare le regole di organizzazione e le altre istruzioni impartite dal Titolare in merito alla collocazione ed all'accesso agli archivi ed al compimento delle operazioni di trattamento sui dati personali, avvisandolo qualora riscontri che taluna di dette regole e/o istruzioni possano contrastare con le norme del GDPR o della legislazione nazionale;
- e) rispettare le regole di raccolta, archiviazione, conservazione e di ogni altro trattamento dei dati disposte dal Titolare, nonché in particolare assicurarsi che il modulo di informativa



e consenso sia reso agli Interessati, ad eccezione dei casi in cui competa direttamente al Titolare medesimo predisporre e controllare l'adempimento alle prescrizioni di legge in tema di informativa e consenso;

- f) incaricare per iscritto i soggetti autorizzati a compiere operazioni di trattamento in nome e per conto del Responsabile e sotto la sua diretta supervisione e responsabilità, fornendo ai medesimi istruzioni operative per una corretta gestione del trattamento nel rispetto dei diritti degli Interessati;
- g) il responsabile si impegna, con riferimento ai propri dipendenti, a dare attuazione a quanto previsto nel Provvedimento Generale del Garante del 27 novembre 2008 e s.m.i. per l'attribuzione del ruolo di Amministratore di sistema. In particolare, il Responsabile deve nominare per iscritto e in modo individuale le persone fisiche incaricate della gestione e manutenzione del sistema informativo, indicando i rispettivi ambiti di competenza e le funzioni attribuite a ciascuno;
- h) eseguire la valutazione di impatto ai sensi dell'art. 35 GDPR ogni qualvolta si renda necessario, nonché avvisare il Titolare della necessità di avviare la consultazione preventiva dell'Autorità di controllo nei casi previsti dall'art. 36 GDPR ovvero richiederne l'autorizzazione in tutti i casi in cui ciò sia previsto, ovvero avviarla o richiederla esso stesso laddove ciò rappresenti un proprio obbligo diretto;
- i) redigere e mantenere un aggiornato registro dei trattamenti ai sensi dell'art. 30 GDPR, secondo le regole del presente Contratto;
- j) laddove necessario, cooperare per l'adozione delle misure di reazione e di notifica nel caso di violazione di dati personali (data breach), ai sensi degli artt. 33 e 34 GDPR, secondo le regole del presente Contratto;
- k) collaborare con gli altri responsabili del trattamento e/o con i contitolari del trattamento;
- l) collaborare con il Responsabile della protezione dei dati (RPD) eventualmente nominato dal Titolare, nonché provvedere a nominare il proprio RPD nei casi previsti dal GDPR dandone pronta comunicazione al Titolare;
- m) osservare le misure di sicurezza già adottate dal Titolare ed adottarne in proprio di idonee come da disposizione che segue;
- n) assistere il Titolare nella soddisfazione delle richieste che gli Interessati avanzino nell'esercizio dei diritti conferiti dal GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile;



- o) effettuare la comunicazione dei dati personali a Destinatari, laddove prevista, solo nei limiti consentiti dalle finalità del trattamento, dal contenuto del consenso prestato dall'Interessato, da disposizioni di contratto o di legge o da altre previsioni analoghe;
- p) laddove la comunicazione abbia ad oggetto Destinatari aventi sede al di fuori dell'Unione Europea, assicurarsi che tali Destinatari aderiscano a regole convenzionali o di autodisciplina nel rispetto dei diritti degli Interessati;
- q) evitare qualsiasi diffusione dei dati personali;
- r) rivolgersi al Titolare per ogni dubbio o chiarimento in merito all'applicazione e all'interpretazione delle disposizioni del GDPR e del presente Contratto, nonché della modulistica privacy adottata (informativa, consenso e simili);
- s) segnalare al Titolare qualunque azione o evento possa costituire o causare un rischio per la conservazione dei dati o la loro integrità, adottando allo stesso tempo tutte le misure idonee ad evitare conseguenze pregiudizievoli al trattamento dei dati;
- t) conservare, aggiornare e mettere a disposizione del Titolare e/o degli organi di controllo, l'elenco con i dati (nome, cognome, funzione e /o ambito di competenza) degli amministratori di sistema nominati e muniti dei necessari requisiti di esperienza, capacità ed affidabilità in conformità di quanto previsto dal Provvedimento 27 novembre 2008 del Garante per la protezione dei dati personali e s.m.i. e curare l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;
- u) adoperarsi in ogni altro modo e adottare ogni altra misura sia idonea per garantire il massimo rispetto dei diritti degli Interessati.

Nell'ambito di quanto sopra, il Responsabile si impegna a cooperare con il Titolare in qualsiasi momento al fine di assicurare il corretto trattamento dei Dati Personali e si impegna a fornire al Titolare tutte le informazioni o i documenti, che potranno essere richiesti da quest'ultima per l'adempimento degli obblighi di legge e per comprovare l'adozione di misure tecniche e organizzative adeguate, entro 10 giorni lavorativi dalla richiesta formulata dal Titolare a mezzo posta elettronica.

6. Condizioni particolari per il caso di violazioni dei dati personali (data breach)

In caso di violazione dei dati personali consistente nella 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 personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve:



- Informare il Titolare tempestivamente e in ogni caso al massimo entro e non oltre 24 ore dalla scoperta dell'evento, di ogni violazione dei dati personali trattati per conto del Titolare che presenti un rischio per i diritti e le libertà delle persone fisiche, indicando il Responsabile della Protezione dei dati (RPD) e relativi dati di contatto;
- nelle successive 24 ore fornire tutti i dettagli completi della violazione subita: in particolare, fornendo una descrizione della natura della violazione dei dati personali, le circostanze in cui è avvenuta, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli interessati coinvolti, i provvedimenti adottati (o che si intendono adottare) per porvi rimedio o comunque mitigarne i possibili effetti negativi;
- attivarsi per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare e attuando tempestivamente tutte le azioni correttive approvate e/o richieste dalla stessa;
- fornire assistenza al Titolare per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti.

7. Documentazione Privacy

Il Responsabile si impegna ad adottare la documentazione in materia di protezione dei Dati Personali prevista dalla normativa italiana ed europea e le relative procedure concernenti le adeguate misure tecniche e organizzative.

8. Condizioni particolari per il riscontro alle istanze degli Interessati

Tenendo conto della natura del trattamento, il Responsabile si obbliga ad assistere e supportare il Titolare del Trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare riscontro alle richieste per l'esercizio dei diritti dell'interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il **[ragione sociale]**) nel rispetto dei termini previsti dall'art. 12 del GDPR.

In particolare, qualora il Responsabile riceva richieste provenienti dagli Interessati, finalizzate all'esercizio dei propri diritti, esso dovrà:

- darne tempestiva comunicazione scritta al Titolare a mezzo posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni designate dal Titolare per gestire le relazioni con gli Interessati;



9. Condizioni particolari per l'adozione delle misure di sicurezza

Il Titolare ha adottato una serie di misure di sicurezza dirette a garantire la riservatezza dei dati personali in suo possesso e ad impedirne l'alterazione, la cancellazione, la distruzione, l'accesso non autorizzato o il trattamento non consentito o non conforme alle finalità della raccolta, nonché a ridurre ogni ulteriore rischio di trattamento illecito dei dati.

A tale fine il Responsabile è tenuto alla stretta osservanza di tali misure di sicurezza come da direttive ricevute e, comunque, a prevederne di proprie in modo idoneo a garantire il rispetto delle previsioni del GDPR e della normativa nazionale applicabile.

In particolare, 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 si impegna a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali; a tale scopo le parti individuano le linee guida di cui all'Opinion 5/2014 del WP29, le linee guida di cui al saggio pubblicato in cooperazione tra l'autorità garante spagnola (AEPD) ed il garante europeo (EDPS), gli standard ENISA ed ogni altro documento equipollente, quali documenti di riferimento per l'elaborazione delle migliori strategie di pseudonimizzazione e cifratura dei dati; restano salvi i casi in cui i dati debbano viceversa essere anonimizzati, per i quali il Responsabile dovrà dare debita e specifica garanzia;
- 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.

Il Responsabile si impegna in particolare ad eseguire operazioni di trattamento solo per il tramite di propri Incaricati appositamente designati e debitamente formati ed istruiti all'adozione ed osservanza delle suddette misure di sicurezza.

A titolo esemplificativo, il Responsabile garantisce che:

- i dati siano in ogni caso trattati dal Responsabile e dai suoi autorizzati secondo le modalità strettamente necessarie allo svolgimento del rapporto, attraverso strumenti tanto informatici e telematici, quanto cartacei;
- il Responsabile ed i suoi Incaricati portino all'esterno della propria sede i dati personali degli Interessati soltanto temporaneamente ed all'esclusivo fine dello svolgimento delle funzioni inerenti il Rapporto;



- per l'uso degli elaboratori elettronici (PC desktop, laptop, mobile device e simili) il Responsabile doti la propria struttura ed i propri autorizzati di credenziali di identificazione ed autenticazione idonei allo scopo.

Per l'elencazione delle misure di sicurezza adottate dal Responsabile si rinvia a separato documento.

10. Sub-Responsabili

Il Responsabile del Trattamento si obbliga, in caso di autorizzazione scritta generale, ad informare il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sub-Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Il Responsabile del Trattamento può comunicare o rendere disponibili i Dati Personali trattati per conto del Titolare esclusivamente ai Sub-fornitori *previamente autorizzati* per iscritto dal Titolare.

Il Responsabile del Trattamento si obbliga a designare detti eventuali Sub-fornitori *previamente autorizzati* quali Sub-Responsabili e a far assumere agli stessi, i medesimi obblighi in materia di protezione dei dati personali cui si è impegnato quale Responsabile del trattamento dati con il presente atto, mediante sottoscrizione di appositi atti giuridici o contratti.

Il Responsabile del Trattamento si obbliga ad informare il Titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Sub-Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche;

Il Responsabile del Trattamento è tenuto ad impartire ai Sub-Responsabili precise istruzioni relativamente al Trattamento oggetto del Contratto e ad assicurarsi che offrano le medesime garanzie in materia di misure tecniche e organizzative previste dal GDPR.

I Sub-Responsabili potranno trattare i Dati Personali nella misura in cui tale trattamento sia strettamente necessario per l'esecuzione del contratto che il Responsabile del Trattamento ha stipulato con il Titolare e in ogni caso nel rispetto del presente contratto.

Qualora il Sub-Responsabile del trattamento designato dall'odierno Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'odierno Responsabile conserva, nei confronti del Titolare del trattamento, l'intera responsabilità dell'adempimento di tali obblighi;

Relativamente al presente accordo, il Responsabile del trattamento **affida/non affida** a Sub-Responsabili, suoi ulteriori fornitori, delle attività che implicino il trattamento di dati personali.



(N.B. Nel caso in cui vi siano Sub-Responsabili è necessario indicarli nella seguente tabella. La stessa tabella è modificabile in base ad esigenze specifiche)

ID	Ragione Sociale	Sede Legale	E-mail/pec	Recapito del DPO	Ambito di trattamento
1					
2					
3					

11. Controlli e attività di audit

Il Responsabile si impegna a consentire al Titolare la verifica del rispetto del presente atto di designazione, a supervisionare e controllare direttamente i soggetti da esso designati per le operazioni di Trattamento ed a tal fine potrà organizzare corsi di formazione. Dette attività di verifica dovranno essere eseguite senza pregiudizio delle normali attività, in orari da concordare e con modalità che consentano il rispetto degli obblighi di riservatezza e confidenzialità nei confronti di altri soggetti e che in ogni caso non ledano o mettano in alcun modo in pericolo i segreti aziendali del [ragione sociale] e/o il suo *know how*. In alternativa, per l'esecuzione delle predette verifiche, il Responsabile potrà avvalersi di soggetti esterni di comprovata esperienza e trasmettere le risultanze al Titolare.

Qualora venga rilevato che un'istruzione impartita dal Titolare violi le disposizioni normative in materia di protezione dei dati personali, il Responsabile si obbliga ad informarne immediatamente il Titolare.

Il Responsabile del Trattamento inoltre riconosce al Titolare il diritto di effettuare controlli (audit) preliminarmente concordati e pianificati relativamente alle operazioni aventi ad oggetto il Trattamento dei Dati Personali del Titolare.

A tal fine, il Titolare potrà periodicamente sottoporre al Responsabile del Trattamento un questionario sul livello di sicurezza e conformità alla normativa in materia di protezione dei dati personali (che dovrà essere debitamente compilato e restituito in tempi brevi) e ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.

Anche per le finalità sopra esposte, il Responsabile è obbligato a mettere a disposizione in qualunque momento e su richiesta del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina ed è altresì



tenuto a contribuire alle attività di revisione realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato, comprese le ispezioni.

I controlli saranno effettuati dal Titolare in base a metodologie concordate tra le Parti.

12. Durata e Cessazione del Trattamento

La presente nomina ha la medesima durata ed efficacia del Contratto e, pertanto, cesserà al momento del completo adempimento o dello scioglimento del vincolo contrattuale, qualsiasi ne sia il motivo. Il trattamento, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato.

A seguito della cessazione del trattamento affidato al Responsabile o nei casi di cui al comma precedente, qualsiasi ne sia la causa, il [ragione sociale] sarà tenuto, a scelta del Titolare e sulla base delle istruzioni dallo stesso impartite, a:

- (i) restituire al Titolare i Dati Personali trattati, con impegno alla rimozione integrale dei dati dal proprio server, oppure
- (ii) provvedere alla loro integrale distruzione (eventuali copie comprese), salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità (contabili, fiscali, ecc.) o il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario. In tal caso il [ragione sociale] dovrà indicare al Titolare i motivi ed i criteri di conservazione dei dati.

13. Condizioni particolari per il trasferimento dei dati all'estero

Il Responsabile si impegna a limitare gli ambiti di circolazione e trattamento dei Dati Personali (es. *memorizzazione, archiviazione e conservazione dei dati sui propri server o in cloud*) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal GDPR (Paese terzo giudicato adeguato dalla Commissione europea, BCR di gruppo, clausole contrattuali modello, etc.).

Il Responsabile, pertanto, non potrà mai trasferire o effettuare il trattamento dei Dati Personali del Titolare al di fuori dell'Unione Europea, in assenza di autorizzazione scritta del Titolare stesso. Qualora il Titolare rilasci l'autorizzazione e sia pertanto effettuato un trasferimento dei Dati Personali del Titolare al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare quanto disposto dal GDPR in materia.



Resta inteso tra le Parti che il Responsabile dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione, consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata del presente Contratto.

Il Responsabile è obbligato a comunicare immediatamente al Titolare il verificarsi di una delle seguenti fattispecie:

- a. mancato rispetto delle clausole contrattuali standard di cui sopra, oppure
- b. qualsiasi modifica della metodologia e delle finalità trasferimento dei Dati Personali del Titolare all'estero.

14. Responsabilità per violazione delle disposizioni

Il Responsabile, con l'accettazione della presente nomina, si impegna a mantenere indenne il Titolare da qualsiasi responsabilità, danno, incluse le spese legali, o altro onere che possa derivare da pretese, azioni o procedimenti avanzati da terzi a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento dei Dati Personali, o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento che sia imputabile a fatto, comportamento o omissione, ivi incluse le eventuali sanzioni che dovessero essere applicate ai sensi del GDPR. Qualora il Titolare e il Responsabile siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato al trattamento, entrambi risponderanno in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

In caso di violazione delle disposizioni contenute nel presente atto relativamente alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute o in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile del trattamento dei dati dal GDPR, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà personalmente e direttamente.

15. Disposizioni finali

Si dà atto che alla scadenza o cessazione del Contratto, per qualsiasi causa, il Responsabile è comunque tenuto all'obbligo di riservatezza.



Qualora una o più delle clausole previste nel presente accordo siano o divengano nulle per forza di legge ovvero a fronte di una decisione del giudice, la validità delle altre disposizioni non sarà in alcun modo pregiudicata.

Il presente Atto viene assoggettato ad imposta di bollo ai sensi dell'art. 18, comma 10, del decreto legislativo 31 marzo 2023, n° 36.

Data _____

Il Titolare del trattamento

Per integrale accettazione

Data _____

Il Responsabile del trattamento
