

Atto di nomina del Responsabile Esterno del Trattamento dei Dati
ai sensi degli art. 28 del Reg. UE 2016/679 ("GDPR")

L'Azienda Ospedaliera di Perugia (C.F. - P. IVA 02101050546), con sede legale in Perugia, in persona del legale rappresentante pro tempore, Ente da qui in avanti indicato come "**Titolare del Trattamento**" dei dati personali,

- visto che l'Azienda Sanitaria di Perugia, in qualità di Titolare del Trattamento ai sensi dell'Art. 4, par. 1, n.° 7) dell'intestato Regolamento (c.d. "GDPR"), intende avvalersi della facoltà di nomina di responsabili esterni dei propri trattamenti ex art. 28 GDPR;

- vista la designazione a Responsabile interno, relativamente ai trattamenti effettuati all'interno della Struttura Complessa sopra indicata;

- visto che con la Ditta nominanda sussiste rapporto di fornitura come da **Determina n.° _____ del _____**, comportante trattamento di dati personali da effettuarsi per conto del Titolare del Trattamento, come meglio precisato nella successiva tabella;

- considerata la particolare natura del contratto e l'impatto che le attività di cui al suddetto contratto hanno sul trattamento dei dati personali e ritenuta opportuna e necessaria la nomina della suddetta Ditta a **Responsabile Esterno del Trattamento**;

ai sensi dell'Art. 28 del Reg. U.E. 2016/679

NOMINA

RESPONSABILE ESTERNO DEL TRATTAMENTO

la Ditta _____ (C.F. _____/P.IVA _____), con sede in _____ (____) al civico n.° ____ della _____ (di seguito "Responsabile Esterno", o "Responsabile"), in persona del Legale Rappresentante *pro tempore*.

Con la sottoscrizione per ricevuta ed accettazione del presente atto, da considerarsi *addendum* contrattuale al rapporto già in essere tra le Parti, il Responsabile Esterno:

- accetta, a titolo gratuito, la nomina a Responsabile Esterno dei trattamenti dei dati personali di cui al richiamato contratto e meglio precisati nella seguente tabella:

N.	Descrizione Fornitura	Interessati	Tipologia dati	Finalità del trattamento	Modalità del trattamento
1	<i>Fornitura di</i> _____ _____ _____ _____ _____	<i>Pazienti c/o Azienda Ospedaliera di Perugia</i>	<i>Anagrafici e sanitari</i>	<i>Istituzionali di cura e ricerca</i>	<i>Cartaceo e digitale</i>

- conferma la sua diretta nonché approfondita conoscenza degli obblighi che assume in relazione a quanto disposto dal Codice Privacy (D.Lgs. n. 196/2003 modificato dal D.Lgs. n. 101/2018) e dal GDPR e

- dichiara di essere in possesso dei requisiti e delle capacità sufficienti a garantire l'adozione di misure tecniche e organizzative adeguate, in modo tale che il trattamento dei dati personali e dei dati appartenenti alle categorie particolari soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati (art. 28, par. 1 GDPR).

In qualità di Responsabile del trattamento, dovrà:

- osservare quanto disposto dalla vigente normativa in tema di protezione dei dati personali ed in particolare dal D. Lgs. 196/2003, dal Reg. UE 2016/679, dai provvedimenti del Garante della Privacy, dalle istruzioni impartite sia nel presente atto, sia in successive ed eventuali comunicazioni della Titolare del Trattamento

(art. 28, par. 1 GDPR). Ove rilevi la propria impossibilità a rispettare tali istruzioni, anche a causa del caso fortuito o della forza maggiore (quali danneggiamenti, anomalie di funzionamento delle protezioni e controllo accessi, ecc.) sarà obbligato ad avvertire immediatamente la Titolare nonché adottare le possibili e più ragionevoli misure di tutela dei dati;

- comunicare alla Titolare del trattamento l'elenco di tutti gli eventuali soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di **“Sub-Responsabili”** per la cui nomina si fornisce espressa **autorizzazione scritta generale**. La Titolare del trattamento potrà verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione generale qui concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla Titolare del trattamento al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali. Il Responsabile del trattamento deve individuare e nominare in forma scritta i propri sub-responsabili. L'atto di nomina/individuazione dovrà riproporre a carico del Sub-Responsabile i medesimi obblighi posti a carico del Responsabile e specificati nel presente documento; in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dalla Legge. Qualora i Sub-Responsabili del trattamento omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserverà, nei confronti della Titolare del trattamento, l'intera responsabilità dell'adempimento degli obblighi dei Sub-Responsabili (art. 28, par. 4 GDPR);

- trattare i dati soltanto su istruzione documentata della Titolare del Trattamento, anche in caso di trasferimento dei dati personali verso un Paese terzo o un'Organizzazione internazionale, salvo che lo richieda il diritto dell'UE o nazionale cui risulta essere soggetto il Responsabile del trattamento. In tal caso il medesimo dovrà informare la Titolare del Trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico [art. 28, par. 3, lett. a) GDPR];

- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o che abbiano un obbligo legale di riservatezza [art. 28, par. 3, lett. b) GDPR];

- adottare [art. 28, par. 3, lett. c) GDPR] le misure di sicurezza previste dall'art. 32 GDPR e ritenute idonee a garantire la riservatezza, l'integrità, la disponibilità e la custodia in ogni fase del trattamento dei dati (quali se del caso la pseudonimizzazione e la cifratura dei dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico...), tenendo conto sia della natura, della finalità del trattamento che dei rischi e facendo espresso riferimento alle Misure minime di sicurezza ICT per le Pubbliche Amministrazioni come da Circolare AGID 2017 e s.m.i.;

- tenere conto della natura del trattamento e assistere la Titolare del Trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo di quest'ultima di dare seguito alle richieste per l'esercizio dei diritti dell'interessato previsti dagli artt. 12 – 23 GDPR [art. 28, par. 3, lett. e) GDPR];

- assistere la Titolare del Trattamento allo scopo di garantire il rispetto degli obblighi di cui agli artt. 32 – 36 GDPR (“Sicurezza dei dati personali”), tenendo conto della natura del trattamento e delle informazioni di cui dispone [art. 28, par. 3, lett. f) GDPR];

- cancellare o restituire, su scelta della Titolare del Trattamento, tutti i dati personali al termine della propria prestazione di servizio, e cancellare le copie esistenti, salvo che il diritto dell'Unione o quello nazionale preveda la conservazione di tali dati [art. 28, par. 3, lett. g) GDPR];

- mettere a disposizione della Titolare tutte le informazioni necessarie al fine di dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, nonché consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dalla Titolare del Trattamento o da altro soggetto da questa incaricato. Dovrà, inoltre, informare immediatamente la Titolare del Trattamento qualora, a suo parere, un'istruzione violi il GDPR o il Codice Privacy o altre disposizioni relative alla protezione dei dati [art. 28, par. 3, lett. h) GDPR];

- informare la Titolare del Trattamento, senza giustificato ritardo, di ogni violazione dei dati personali (art. 33,

par. 2 GDPR) al fine di consentire alla Titolare stessa il rispetto delle attività di notifica all'Autorità di controllo. La comunicazione dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC ufficiale e dovrà contenere informazioni circa: a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero almeno approssimativo di interessati in questione, nonché le categorie e il numero almeno approssimativo di registrazione dei dati personali in questione; b) il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni; c) la descrizione delle probabili conseguenze della violazione dei dati personali; d) la descrizione delle misure adottate da parte del Responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi. Il Responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite;

- tenere il Registro delle Attività di Trattamento dei dati, svolte sotto la propria responsabilità (art. 30 GDPR) ed esibirlo a richiesta dalla Titolare del Trattamento;

- cooperare con l'Autorità di controllo nell'esecuzione dei suoi compiti (art. 31 GDPR);

- trattare i dati nel rispetto dei principi di liceità, correttezza, trasparenza, legittimità, esattezza, aggiornamento, pertinenza, non eccedenza, completezza, adeguatezza e conservazione, limitatamente al conseguimento della finalità che il suo incarico prevede e nell'osservanza di quanto disposto dagli artt. 1, 2-decies del nuovo Codice Privacy e 5 del GDPR (minimizzazione dei dati);

La presente nomina è condizionata, per oggetto, durata, natura e finalità del trattamento, nonché per il tipo di dati personali, per le categorie di interessati, per gli obblighi e i diritti della Titolare del trattamento al contratto di cui in premessa (in fase di esecuzione) e si intenderà revocata di diritto contestualmente alla cessazione o alla risoluzione dello stesso.

Perugia, li _____

Dott. Giuseppe De Filippis (n.q.) _____

Per presa visione e accettazione.

Il Responsabile del trattamento _____