

## **ALLEGATO**

### **NOMINA RESPONSABILE PER IL TRATTAMENTO DI DATI PERSONALI ai sensi e per gli effetti dell'art. 28 Reg UE 2016/679 del 27/04/2016**

La **Azienda Sanitaria Locale CN2 (ASL CN2)**, con sede legale in Via Vida, 10 – 12051 ALBA (CN), in persona del legale rappresentante p.t., quale Titolare del trattamento dei dati personali e/o particolari, ai sensi dell'art. 28 del Regolamento UE/2016/679 (di seguito, anche, "GDPR")

#### **PREMESSO CHE**

- L'ASL CN2 ha affidato l'incarico di [indicare tipologia di incarico] a [indicare ragione sociale, sede legale, partita iva del Responsabile];
- L'affidamento dell'incarico di cui sopra comporta lo svolgimento in capo a [indicare ragione sociale del Responsabile] del/i compito/i di: [indicare le attività affidate che l'ente affidatario deve svolgere];
- Lo svolgimento delle attività/dei servizi sopra descritte/i comporta il trattamento di dati personali nella titolarità dell'ASL CN2;
- [indicare ragione sociale del Responsabile] assicura che nello svolgimento di tali attività/servizi adotta tutte le misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato (art. 28 par. 1);
- Le parti del presente contratto per l'affidamento del suddetto incarico sono consapevoli dell'importanza della protezione dei dati personali e dichiarano di essere a conoscenza di quanto prescritto dalle disposizioni normative loro applicabili in materia di protezione dei dati;

#### **NOMINA**

[indicare ragione sociale, sede legale, partita iva del Responsabile]

quale

#### **RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI**

Il presente documento rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dall'art. 28 par. 3 del GDPR.

#### **AMBITO DI APPLICAZIONE**

## **Clausola 1 - Descrizione del trattamento**

- a) Il Responsabile del trattamento esegue le operazioni di trattamento dei dati personali ad esso delegate in accordo alle istruzioni, generali e specifiche, fornite dal Titolare.
- b) I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del Titolare del trattamento, sono specificati nell'**Allegato I**.
- c) la nomina a Responsabile del trattamento di cui al Contratto comprende il trattamento di dati personali che il Responsabile svolge per conto del Titolare, sia quando quest'ultimo agisce in qualità di Titolare del trattamento, sia quando essa agisce in qualità di Responsabile del trattamento; in tali casi, il Fornitore opererà quale sub-responsabile del trattamento e il termine "Responsabile" utilizzato nella Contratto dovrà intendersi quale "Sub-responsabile" e il termine "Titolare" dovrà intendersi quale "Responsabile".

## **Clausola 2 – Prescrizioni a carico del Responsabile del trattamento**

### **2.1. Istruzioni**

- a) Il Responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, 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 lo vietи per rilevanti motivi di interesse pubblico. Il Titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.
- b) Il Responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

### **2.2. Limitazione delle finalità**

Il Responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'**Allegato II**, salvo ulteriori istruzioni del Titolare del trattamento.

### **2.3. Durata del trattamento dei dati personali e conservazione**

- a) Il Responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'**Allegato I**.
- b) Al termine del contratto, il Responsabile ha l'obbligo di cancellare o restituire al Titolare del trattamento i dati personali trattati sulla base delle indicazioni e delle scelte comunicate dal Titolare del trattamento.
- c) Il Responsabile ha inoltre l'obbligo di cancellare tutte le copie esistenti dei dati oggetto del trattamento dopo la scadenza dei tempi di conservazione definiti, a meno che il diritto UE o il diritto nazionale ne preveda la conservazione ulteriore.

### **2.4. Sicurezza del trattamento**

- a) Il Responsabile del trattamento adotta tutte le misure tecniche e organizzative idonee a garantire la sicurezza del trattamento con particolare riferimento allo specifico rischio connesso alla tipologia di dati trattati, così come previsto dall'art. 32 GDPR.
- b) Nello specifico, il Responsabile deve:
  - ove possibile e proporzionale al trattamento eseguito, adottare tecniche di pseudonimizzazione o cifratura dei dati personali;
  - garantire su base permanente la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di trattamento;
  - garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - garantire la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- c) Il Responsabile si impegna, pertanto, ad adottare – prima dell'avvio del trattamento ad esso delegato dal Titolare – le misure di sicurezza, tecniche ed organizzative, dettagliate nell'**Allegato II** del presente atto di nomina.
- d) Il Responsabile si impegna inoltre a mantenere le suddette misure in vigore per tutto il tempo del trattamento e di aggiornarne il contenuto, ove il trattamento richieda misure più stringenti o renda applicabili misure alternative, purché idonee a garantire un livello di sicurezza adeguato agli standard dei cui all'art. 32 GDPR. Il Responsabile si impegna ad avvisare il Titolare di ogni modifica apportata alle misure adottate.
- e) Il Responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento al solo personale autorizzato soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

## **2.6. Documentazione e rispetto**

- a) Il Responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del Titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.
- b) Il Responsabile del trattamento mette a disposizione del Titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679.
- c) Su richiesta del titolare del trattamento, il Responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

- d) Il Titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente purchè non concorrente del Fornitore. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole di almeno 15 giorni.

## 2.7. Ricorso a sub-responsabili del trattamento

- a) Con la presente nomina si fornisce espressa autorizzazione scritta generale all'individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub responsabili".
- b) Il Responsabile del trattamento è tenuto a nominare per iscritto i sub-responsabili di cui si avvale e a comunicare al Titolare l'elenco di tutti i soggetti individuati (**Allegato III**).
- c) Qualora il Responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al Responsabile del trattamento conformemente alle presenti clausole. Il Responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.
- d) Su richiesta del Titolare del trattamento, il Responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.
- e) Il Responsabile del trattamento rimane pienamente responsabile nei confronti del Titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il Responsabile del trattamento. Il Responsabile del trattamento notifica al Titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

## 2.8. Trasferimenti extra-UE

In caso di trasferimento di dati verso un Paese terzo o una organizzazione internazionale, fatte salve le ipotesi in cui il Responsabile debba adempiere ad un obbligo imposto dal diritto UE o dal diritto nazionale, esso dovrà richiedere espressa e specifica autorizzazione al Titolare del trattamento e garantire che il trasferimento avvenga in sussistenza di almeno una delle condizioni di legittimità previste dal GDPR.

## Clausola 3 - Assistenza al Titolare del trattamento

### 3.1. Diritti degli interessati

- a) Il Responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato.

- b) Il Responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento.
- c) Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

### **3.2. DPIA**

- a) Il Responsabile del trattamento assiste il Titolare del trattamento nel garantire il rispetto dell'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati» o «DPIA») qualora un tipo di trattamento che coinvolge anche il Responsabile possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- b) Il Responsabile supporta, inoltre, il Titolare nell'eventuale fase di consultazione dell'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento in cui è previsto il suo coinvolgimento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

### **3.3. Rapporti con l'Autorità**

Il Responsabile supporta il Titolare nella gestione dei rapporti con l'Autorità, attraverso l'invio, senza ingiustificato ritardo, delle informazioni richieste e dei documenti relativi alle misure adottate.

### **Clausola 4 - Notifica di una violazione dei dati personali**

- a) In caso di violazione dei dati personali, il Responsabile del trattamento coopera con il Titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.
- b) Il Responsabile ha l'obbligo di informare il Titolare senza ingiustificato ritardo di ogni violazione, anche potenziale, dei dati personali trattati per suo conto, specificando la natura della violazione, le categorie ed il numero di dati ed interessati coinvolti (da intendersi come tale la 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).
- c) È, altresì, fatto obbligo al Responsabile di adottare tempestivamente tutte le misure idonee e necessarie a porre rimedio alla violazione o limitare i danni dalla stessa prodotti per gli interessati.

### **Clausola 5 - Inosservanza delle clausole e risoluzione**

- a) Le Parti del presente Atto sono soggette, da parte dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Ferma restando l'applicazione di tale norma e, in generale, della Normativa Privacy, il mancato rispetto delle funzioni delegate e delle istruzioni impartite al Responsabile ovvero la violazione delle condizioni prescritte, darà luogo all'applicazione di penali e/o alla risoluzione del rapporto principale.
- b) Il Responsabile assume piena responsabilità diretta verso gli interessati solo se non ha adempiuto gli obblighi dalla Nomina Privacy o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
- c) Fermo restando quanto previsto dall'art. 82 GDPR, il Responsabile si impegna a manlevare il Titolare e tenere quest'ultimo indenne da qualsiasi tipo di conseguenza, sia civile sia amministrativa, responsabilità, perdita, onere, spesa, danno o costo da quest'ultimo sopportato che sia la conseguenza di condotte, anche omissive, imputabili al Responsabile, ovvero di violazioni agli obblighi o adempimenti prescritti dalla Normativa Privacy ovvero di inadempimento delle pattuizioni contenute nel presente Atto di nomina, ovvero dei compiti assegnati dal Titolare.
- d) Inoltre, qualora il Responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il Titolare del trattamento può dare istruzione al Responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il Responsabile del trattamento informa prontamente il Titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
- e) Il Titolare del trattamento ha, pertanto, diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole anche qualora:
- il trattamento dei dati personali da parte del Responsabile del trattamento sia stato sospeso dal Titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
  - il Responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;
  - il Responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.
- f) Dopo la risoluzione del contratto il Responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del Titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al Titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

## Clausola 6 – Durata del trattamento e della nomina

Il presente Atto produce i suoi effetti a partire dalla data di sottoscrizione delle Parti e rimarrà in vigore fino alla cessazione delle attività svolte dal Responsabile a favore del Titolare, indipendentemente dalla causa di detta cessazione.

Il Trattamento, fatto salvo ogni eventuale obbligo di legge e/o contenzioso, avrà una durata non superiore a quella necessaria al raggiungimento delle finalità per le quali i dati sono stati raccolti.

\_\_\_\_\_, lì \_\_\_\_\_

Il Titolare del trattamento ASL CN2

Il Responsabile del trattamento \_\_\_\_\_

Dott.ssa Paola MALVASIO

## **ALLEGATO I**

Descrizione del trattamento

Categorie di interessati i cui dati personali sono trattati

- Dipendenti/Collaboratori
  - Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
  - Associati, soci, aderenti, simpatizzanti, sostenitori
  - Soggetti che ricoprono cariche sociali
  - Beneficiari o assistiti
  - Pazienti
  - Minori
  - Persone vulnerabili (es. vittime di violenza o abusi, rifugiati, richiedenti asilo)
  - Altro
- .....

Dati sensibili trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

- Dati che rilevano l'origine razziale o etnici
- Dati relativi a opinioni politiche

- Dati relativi a convinzioni religiose o filosofiche
- Dati che rivelano l'appartenenza sindacale
- Dati relativi alla vita sessuale o all'orientamento sessuale
- Dati relativi alla salute
- Dati genetici
- Dati biometrici
- Altro

Garanzie applicate:

.....  
.....  
.....  
.....  
.....  
.....  
.....

Natura del trattamento:

- Informatico – con strumenti digitali
- Cartaceo/documentale
- Verbale (mera consultazione)
- Altro .....

Località del trattamento

.....  
.....  
.....  
.....  
.....  
.....  
.....

Durata del trattamento

.....  
.....  
.....  
.....  
.....

## **ALLEGATO II**

In qualità di Responsabile il fornitore è tenuto a rispettare le seguenti misure di sicurezza minime:

- o Elaborazione di procedure e policy di sicurezza logiche e fisiche;
- o Sistemi di identificazione, autenticazione e autorizzazione;
- o Livelli di accesso alle cartelle di rete differenziati in base alle mansioni di ciascun collaboratore (Profilazione utenti);
- o Antivirus, antispam, firewall;
- o Backup;
- o Modalità tecniche di ripristino dei dati in caso di accidentale distruzione o alterazione (Dysaster recovery, Business Continuity);
- o Sistemi di crittografia o pseudonimizzazione.

Descrizione delle misure tecniche e organizzative specifiche che il responsabile del trattamento deve prendere per essere in grado di fornire assistenza per il titolare del trattamento in particolare **per le ditte di informatica o per forniture di software e/o di apparecchiature (compresi apparecchiature medicali) con hardware e software che si interfacciano con la rete informatica dell'ASL CN2:**

Il “Responsabile esterno” deve:

- mettere in atto le misure tecniche e organizzative previste dall’Allegato “Piano Aziendale misure di sicurezza ICT (AGID)- Prescrizioni per fornitori”;
- mettere in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati (privacy by design);
- mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica attività del trattamento, con riferimento alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all’accessibilità (privacy by default);
- se esercitano funzioni di Amministratore di sistema ai sensi del Provvedimento del Garante **“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 e ss.mm.ii.”**, deve essere compilato e sottoscritto il modello “Amministratore di sistema” allegato;

**Nel caso in cui il contratto abbia ad oggetto la consegna dei presidi sanitari al domicilio dell’interessato inserire altresì le seguenti istruzioni:**

Il “Responsabile esterno” deve:

- attenersi alle disposizioni previste dai provvedimenti del Garante per la protezione dei dati personali del 09 novembre 2005 rubricato “Strutture sanitarie: rispetto della dignità” e n. 520 del 21 novembre 2013 nella consegna dei presidi sanitari al domicilio degli interessati, si ricorda in particolare che:

- la consegna deve avvenire
  - nel luogo individuato dall'interessato rispettando gli orari scelti da quest'ultimo tra quelli indicati dall'ASL titolare del trattamento;
  - preferibilmente nelle mani dell'interessato; il presidio non può essere lasciato incustodito nelle vicinanze del luogo indicato dall'interessato;
- Il presidio, laddove le dimensioni e la natura lo consentano, deve essere, in ogni caso, imballato in un contenitore non trasparente che non deve contenere nella parte esterna l'indicazione del contenuto;
- Il presidio può essere consegnato a terzi (ad es. vicino di casa, parente, portiere) solo su espressa indicazione dell'interessato. Nel caso in cui l'interessato, o il terzo delegato da questo, non siano presenti al momento della consegna, il personale aa ciò deputato deve lasciare esclusivamente un avviso che non contenga l'indicazione della tipologia del presidio. Il personale deputato alla consegna non deve indossare divise recanti scritte da cui si possa evincere la specifica tipologia dei presidi in consegna, né utilizzare automezzi recanti tali scritte.

### **ALLEGATO III**

Elenco dei sub-responsabili del trattamento

Sub-responsabile <i>(Nome, ragione sociale, sede legale)</i>	Luogo di trattamento <i>(Luogo in cui il trattamento è effettivamente eseguito)</i>	Attività delegate