ACCORDO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679 del 27 aprile 2016

Tra

– **Azienda Socio Sanitaria Territoriale (ASST) di Mantova,** di seguito anche "**Ente Sanitario**", codice fiscale n. 02481840201, con sede in Mantova, Strada Lago Paiolo n. 10, nella persona del legale rappresentante pro tempore;

E

– **Azienda Regionale per l'Innovazione e gli Acquisti S.p.A.,** di seguito anche "**ARIA S.p.A.**", codice fiscale n. 05017630152, con sede in Milano, via T. Taramelli n. 26, nella persona del legale rappresentante/delegato pro tempore, domiciliato per la carica in Milano, via T. Taramelli n. 26;

di seguito ciascuna indicate, individualmente "la Parte" e collettivamente "le Parti".

PREMESSO CHE

1. ASST di Mantova (di seguito "Titolare del trattamento") per la quale ARIA S.p.A. assume la veste di Responsabile del trattamento di dati personali in virtù della stipula di separati accordi, è Titolare del trattamento dei dati personali per finalità istituzionali, secondo la definizione dell'art. 4, par. 1, n. 7 del Regolamento UE 2016/679;
2. ASST di Mantova ha individuato, ARIA S.p.A. come Responsabile del trattamento, in quanto la stessa presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo che il trattamento rispetti i requisiti della normativa e la tutela degli interessati (art. 32 Regolamento UE 679/2016);
3. Ai sensi dell'art. 28 del Regolamento UE 2016/679, il Titolare del trattamento ha la facoltà di autorizzare il Responsabile ad avvalersi di Ulteriori Responsabili del trattamento, salvo l'obbligo in capo al Responsabile di informare il Titolare del trattamento della nomina rilasciata ed il diritto di quest'ultimo a manifestare la propria opposizione;

Tutto ciò premesso, le Parti

CONCORDANO E STIPULANO QUANTO SEGUE:

1. DEFINIZIONI

Ai fini del presente Atto di nomina valgono le seguenti definizioni:

- **Per "Legge Applicabile" o "Normativa privacy":** si intende 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 (di seguito per brevità "GDPR"), il D. Lgs. N. 196/2003 modificato dal D.Lgs. N° 101 del 10 agosto 2018, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile all'interno del territorio nazionale, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali.
- **Per Trattamento:** si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.
- **Per "Dati Personali":** si intendono tutte le informazioni così come definite ai sensi dell'art. 4 par. 1 del GDPR, che il Responsabile del trattamento tratta per conto del Titolare allo scopo di fornire i Servizi..
- **Per "Servizi":** si intendono i Servizi erogati da Aria nonché il relativo trattamento dei dati personali,

così come meglio descritto nel presente Atto di nomina e nei suoi allegati.

- **Per "Responsabile del Trattamento":** si intende, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
- **Per "Sub-Responsabile":** si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile del trattamento abbia eventualmente affidato parte della prestazione facente parte dei Servizi, e che quindi tratta dati personali, previa autorizzazione del Titolare secondo le modalità di cui all'art. 28 del GDPR e con separato Atto di Nomina da parte del Responsabile del Trattamento.
- **Per "Misure di Sicurezza":** si intendono le misure di sicurezza di cui alla normativa in materia di protezione dei dati personali.
- **Per "Macroarea di Trattamento":** si intende un insieme organizzato di processi di trattamento, riconducibili ad uno o più Servizi, raggruppati o classificati sulla base di determinate caratteristiche o criteri di omogeneità.

2. NOMINA

Aria S.p.A., in relazione a tutti i trattamenti di dati personali resi necessari in attuazione delle attività svolte per conto del Titolare del trattamento, è nominata dal Titolare del Trattamento, come sopra individuato, quale Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

3. OGGETTO

Il Responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui alla presente nomina, salvo ulteriori istruzioni del Titolare del trattamento. Nello specifico Aria S.p.A. effettuerà il trattamento di dati personali necessario, e comunque connesso all'espletamento del Servizio, di seguito individuato:

TRATTAMENTO	CATEGORIE DI DATI TRATTATI	CATEGORIE DI INTERESSATI	DESCRIZIONE DEL TRATTAMENTO	FINALITA' DEL TRATTAMENTO
Sistema Informativo per la gestione dello Screening oncologico alla prostata	D1) Dati comuni: Anagrafici (nome, cognome, codice fiscale, sesso, ATS di assistenza, indirizzo di domicilio e di residenza); D2) Dati comuni di contatto (numero di telefono, indirizzo e-mail); D3) Dati particolari: Sanitari (dati relativi all'anamnesi personale e familiare; dati relativi agli esiti degli accertamenti effettuati).	I1) Cittadini	Il Sistema Informativo per la gestione dello Screening oncologico alla prostata è un'iniziativa rivolta ad uno specifico segmento di popolazione maschile eleggibile per effettuare un'indagine diagnostica che consenta di identificare precocemente i soggetti potenzialmente affetti patologie tumorali alla prostata, offerto dalla Regione Lombardia con DGR n. XII/2767 del 15/07/2024 in considerazione degli obiettivi per garantire il benessere dei cittadini definiti dalla Raccomandazione del Consiglio dell'Unione Europea N°4770/22 (29/11/2023) e dal Piano	F1) Gestione dei dati relativi agli esiti degli accertamenti effettuati dagli assistiti per il perseguimento delle finalità di prevenzione diagnosi e cura nell'ambito dei percorsi diagnostico terapeutici previsti dal programma di screening alla prostata.

			Oncologico Nazionale 2023-2027 di cui all'Intesa, ai sensi dell'articolo 8, comma 6, della legge 5 giugno 2003, n. 131, tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano del 26/01/2023. Lo screening è eseguito da professionisti sanitari.	

Tenuto conto del ruolo del Responsabile e delle caratteristiche dei Servizi erogati nell'interesse di Regione Lombardia e degli Enti territoriali di cui il Titolare fa parte, tenuto in considerazione altresì che tali Servizi sono erogati sulla base di apposite Convenzioni e regolati da atti normativi di diverso rango e in continua evoluzione che ne disciplinano le modalità e le peculiarità, il Titolare e il Responsabile concordano che, in applicazione del principio di accountability, il Responsabile inoltrerà ad ogni modifica rilevante, o su richiesta del Titolare, il dettaglio aggiornato del trattamento di dati personali sopra individuato ai dati di contatto forniti dal Titolare (cfr par. 10 del presente atto).

4. DURATA

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

Le obbligazioni sorte per effetto della stipula del precedente contratto tra le Parti non sono in alcun modo estinte o novate dal presente contratto. In caso di contrasto tra disposizioni contrattuali, prevarranno quelle presenti all'interno del presente atto di nomina.

5. MODALITA' E ISTRUZIONI

Le modalità e le istruzioni per il trattamento dei dati personali impartite dal Titolare del trattamento ad Aria S.p.a. sono specificatamente indicate e declinate nell'Allegato 1 "Misure di Sicurezza", parte integrante e sostanziale del presente Atto di nomina.

6. OBBLIGHI E DOVERI DEL RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento dichiara di avere una struttura ed una organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali del Titolare e si impegna ad adeguarla ovvero a mantenerla adeguata alla rilevanza dell'incarico stesso, garantendo il pieno rispetto (per sé e per i propri dipendenti e collaboratori) delle istruzioni sul trattamento dei dati personali, oltre che di tutte le norme di legge in materia applicabili.
ARIA S.p.A. si obbliga, altresì, a prestare assistenza al Titolare del trattamento, nel garantire il rispetto degli obblighi previsti dagli artt. 33 (Notifica di una violazione dei dati personali all'Autorità di controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato) e 35 (Valutazione di impatto sulla protezione dei dati) del Regolamento Europeo 2016/679, tenendo conto della natura del trattamento e delle informazioni di cui ha la disponibilità.
ARIA S.p.A. si impegna a collaborare attivamente con l'Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, al fine di consentire a queste ultime l'esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi ed ispezioni, relativamente ai trattamenti oggetto dell'atto di nomina.

ARIA S.p.A. si impegna a prestare la propria collaborazione e avvisare prontamente il Titolare, inoltrando la segnalazione ai dati di contatto forniti dal Titolare (cfr par. 10 del presente Atto) nel caso in cui riceva una richiesta dall'interessato in modo tale da agevolare il Titolare del Trattamento nel garantire il

soddisfacimento dei diritti riconosciuti agli interessati dagli artt. 15 – 22 del Regolamento Europeo.

7. NOMINA DI SUB-RESPONSABILI

Ai sensi dell'art. 28 par. 2 del Regolamento UE 2016/679, ARIA S.p.A. in qualità di Responsabile del Trattamento ha l'autorizzazione generale del Titolare del trattamento per ricorrere a sub-responsabili del trattamento per le attività summenzionate, previo esperimento delle necessarie procedure di selezione dei fornitori applicabili di volta in volta.

Tale nomina di un ulteriore Responsabile del trattamento da parte di Aria S.p.a. sarà possibile a condizione che su tale soggetto siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dalle leggi applicabili. Aria S.p.a. rimane tuttavia pienamente responsabile nei confronti del Titolare del trattamento dell'adempimento degli obblighi da parte dell'ulteriore Responsabile del trattamento.

In considerazione del funzionamento e della complessità dell'ecosistema sanitario lombardo, nelle attività di approvvigionamento di beni e servizi informatici inerenti ai trattamenti di cui alla presente nomina, ARIA S.p.A. nella valutazione degli ulteriori responsabili del trattamento terrà sempre in considerazione gli elementi di cybersicurezza come da procedure di gara ad evidenza pubblica commissionate da Regione Lombardia e si impegna a comunicare al Titolare eventuali modifiche a tale elenco, riguardanti l'aggiunta o la sostituzione di ulteriori responsabili del trattamento, con congruo anticipo, dando così al Titolare del trattamento tempo sufficiente per segnalare eventuali punti di attenzione nel rispetto dei principi di correttezza e buona fede previsti dal Codice Civile.

8. VIGILANZA

Come previsto dall'art. 28, par. 3 GDPR, il Responsabile mette a disposizione del Titolare le informazioni necessarie al fine di rilevare il rispetto degli obblighi previsti dalla normativa privacy, in accordo con le modalità e le tempistiche concordate con il Titolare stesso.

Allo scopo di vigilare sulla puntuale osservanza delle istruzioni impartite al Responsabile, il Titolare del trattamento potrà effettuare azioni di verifica. Aria S.p.a. si obbliga ad agevolare l'esecuzione di tali verifiche previa comunicazione da parte del Titolare del trattamento, in accordo con le modalità e le tempistiche concordate tra le Parti. Nell'ambito di tali verifiche, il Responsabile si impegna a fornire l'assistenza ed il supporto necessari, rispondendo alle richieste del Titolare del trattamento in relazione ai dati ed ai trattamenti oggetto degli accordi stipulati tra le Parti.

9. RESPONSABILITÀ PER VIOLAZIONE DELLE DISPOSIZIONI

Conformemente alle prescrizioni di cui all'art. 82 del Regolamento, qui richiamato in toto, Aria S.p.A. in qualità di Responsabile del trattamento dei dati personali risponderà per il danno riconosciuto agli interessati e ad essa imputabile derivante dal mancato adempimento degli obblighi specificatamente diretti al Responsabile del trattamento dei dati dal GDPR o derivante da un trattamento effettuato in difformità rispetto alle legittime istruzioni del Titolare del trattamento. Qualora il Responsabile determini autonomamente le finalità e i mezzi di trattamento in violazione del GDPR o del presente Accordo, sarà considerato a tutti gli effetti Titolare del trattamento.

10. DATI DI CONTATTO

Per le comunicazioni relative alla gestione del presente Atto di nomina fare riferimento ai seguenti punti di contatto presso il Titolare del Trattamento:

– Dati di contatto del titolare del trattamento:

Funzione	Direttore Generale/Legale Rappresentante
E-mail	protocollogenerale@pec.asst-mantova.it
Telefono (facoltativo)	03762011

In caso di incidente di sicurezza e/o data breach fare riferimento a	Struttura Affari Generali e Controlli Interni e-mail: privacy@asst-mantova.it

Per le comunicazioni relative alla gestione del presente Atto di nomina fare riferimento ai seguenti punti di contatto presso il Responsabile del Trattamento:

Funzione	Ufficio Supporto Normativo Protezione dei dati Personali (o Ufficio Privacy)
E-mail	PEC: nomineprivacy@pec.ariaspa.it PEO: uffprivacy.siss@ariaspa.it

Milano, Lì ……..

PER ASST MANTOVA
IL LEGALE RAPPRESENTANTE PRO TEMPORE
Dott.ssa Anna Gerola

PER ARIA S.P.A.
IL LEGALE RAPPRESENTANTE/DELEGATO PRO TEMPORE

Il presente documento è firmato digitalmente dai rappresentanti legali pro tempore di ASST di Mantova e di ARIA S.P.A.

ALLEGATO 1 MISURE DI SICUREZZA

1. AMBITO DI APPLICAZIONE E RIFERIMENTI

Per il Titolare e il Responsabile il presente documento costituisce allegato contrattuale, contenente i requisiti richiesti per una corretta gestione della sicurezza delle informazioni trattate. L'intento perseguito è quello di mettere in sicurezza l'intera catena di fornitura che opera per conto del Titolare, secondo le specifiche normative di settore. Il Titolare e il Responsabile si propongono di costruire un rapporto di fiducia per garantire a tutti gli interessati coinvolti un adeguato livello di protezione dei dati personali.

Il Responsabile del trattamento individuato è tenuto ad effettuare i trattamenti dei dati nel rispetto di quanto disposto dalla Normativa privacy e di ulteriori ed eventuali contenuti specifici dell'atto sottoscritto dalle Parti, secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli Interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il Responsabile è tenuto in modo lecito e secondo correttezza ad applicare e rispettare i Principi previsti dal Regolamento UE 2016/679 (GDPR) quali, ad esempio, il principio di trasparenza, necessità, proporzionalità, pertinenza e non eccedenza. Il Responsabile è tenuto a trattare i dati per scopi legittimi e determinati rispettando il principio di minimizzazione dei dati trattati, principio di privacy by design, limitazione della conservazione, integrità e riservatezza e assicurando l'esattezza e la completezza dei dati in accordo con il principio di accountability. In applicazione del Principio di Limitazione della conservazione, il Responsabile si impegna a rispettare e, ove necessario, implementare il periodo di conservazione dei dati personali definito e comunicatogli dal Titolare o previsto da obblighi di legge a cui il Responsabile o il Titolare sono soggetti.

Il Responsabile è tenuto ad iniziare eventuali nuovi trattamenti relativi ad ulteriori macroaree di trattamento solo in seguito a richiesta da parte del Titolare. In caso di revoca della designazione a Responsabile dei trattamenti, o, in ogni caso, dopo il completamento di un trattamento per conto del Titolare, il Responsabile deve, sulla base delle istruzioni impartite dal Titolare, restituire o cancellare i dati personali, salvo che il diritto dell'Unione o degli Stati membri cui è soggetto, ne prescriva la conservazione.

In tema di sicurezza dei dati personali, ai sensi dell'art. 32 del GDPR, il Responsabile del trattamento è tenuto a mettere in atto misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio. Il Responsabile si impegna ad adottare un approccio alla sicurezza basato sul rischio. Il Responsabile adotta le misure di sicurezza contenute all'interno del presente allegato, tenendo in considerazione il rischio individuato, calcolato in base alla natura, all'oggetto, al contesto e alle finalità del trattamento e a documentare di aver applicato tale approccio in tutte le fasi del trattamento.
Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o 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, o dati relativi a condanne penali e a reati («dati sensibili»), il Responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari in base al rischio individuato.
Nel valutare l'adeguatezza del livello di sicurezza, il Responsabile terrà conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

I requisiti contenuti all'interno del presente allegato risultano conformi alle disposizioni contenute nei seguenti atti normativi e standard internazionali:

- Reg. UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)
- Decreto legislativo 196/03 (Codice in materia di protezione dei dati personali) e ss.mm.ii
- Decreto Legislativo 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale e ss.mm.ii (D. Lgs. 22 agosto 2016 n. 179 e D.Lgs. 13 dicembre 2017 n. 217)
- Decreto-legge 16 luglio 2020, n. 76, «Misure urgenti per la semplificazione e l'innovazione digitale»

e ss.mm.ii

- DPCM n.178 del 29 settembre 2015 «Regolamento in materia di fascicolo sanitario elettronico» e ss.mm.ii
- CIRCOLARE 18 aprile 2017, n. 2/2017. Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» e ss.mm.ii
- Framework Nazionale di Sicurezza Cibernetica FNSC - Allegato B2 alla Determinazione 307/2022 (relativa alla Strategia Cloud Italia) e ss.mm.ii
- Decreto Direttoriale n. 20610 in data 28 luglio 2023 di ACN
- Determinazione del 15 dicembre 2021, n. 628, dell'Agenzia per l'Italia digitale, di adozione del «Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione», di cui è stato dato avviso nella Gazzetta Ufficiale delle Repubblica italiana n. 19 del 25 gennaio 2022 (c.d. regolamento "Cloud della PA");
- Determina del 18 gennaio 2022, n. 306, dell'Agenzia per la cybersicurezza nazionale, recante l'adozione del modello per la predisposizione dell'elenco e della classificazione di dati e di servizi;
- Determina del 18 gennaio 2022, n. 307, dell'Agenzia per la cybersicurezza nazionale, di adozione dell' «Aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa, e affidabilità delle infrastrutture digitali per la pubblica amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi cloud per la pubblica amministrazione, nonché requisiti di qualificazione dei servizi cloud per la pubblica amministrazione»;
- VISTO il decreto del Direttore generale dell'Agenzia per la cybersicurezza nazionale del 2 gennaio 2023, prot. n. 29, recante: «Nuovo processo di qualificazione dei servizi cloud per la pubblica amministrazione»
- Security and Privacy Controls for Information Systems and Organization - NIST_SP_800_53
- Federal Information Processing Standard (FIPS) Publication n. 140-2

2. DEFINIZIONI

Ai fini del presente Allegato valgono le seguenti definizioni:

- **Autenticazione**: la procedura di verifica dell'identità di un utente da parte di un sistema o servizio.
- **Autorizzazione**: la procedura che verifica se un soggetto interno o esterno ha il diritto di compiere una certa azione, ad esempio trasferire fondi o accedere a dati sensibili.
- **Credenziali**: le informazioni – generalmente riservate – utilizzate da un utente a fini di autenticazione ad un sistema o servizio. Sono inclusi nella definizione gli strumenti fisici che forniscono o memorizzano le informazioni (ad es. generatori di password non riutilizzabili o smart card) o qualcosa che l'utente ricorda (ad es. password) o rappresenta (ad es. caratteristiche biometriche).
- **KPI (Key Performance Indicator)**: metriche che indicano il successo di un'attività, focalizzandosi sulle performance passate al fine di promuovere un processo di miglioramento continuo.
- **Minimo privilegio (least privilege)**: il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati.
- **Segregazione dei ruoli (segregation of duties)**: il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite.

3. MISURE DI SICUREZZA

3.1. POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

Il Responsabile è tenuto a garantire l'adozione di politiche in materie di sicurezza delle informazioni e di procedure operative specifiche relative alla sicurezza dei dati personali. Il Responsabile garantisce che tali politiche e procedure siano opportunamente approvate, periodicamente aggiornate e adeguatamente comunicate ai soggetti coinvolti nel trattamento.

3.2. ORGANIZZAZIONE PER LA SICUREZZA

Il Responsabile garantisce di adottare un processo finalizzato alla definizione e assegnazione dei ruoli e delle responsabilità relative al trattamento dei dati personali, coerentemente con quanto definito all'interno della politica di sicurezza adottata. Tale processo garantisce l'assenza di ruoli aziendali in conflitto nell'ambito della protezione dati personali (a titolo esemplificativo, Responsabile dei sistemi informativi e DPO possono essere ruoli in conflitto).

Il Responsabile deve garantire che chi agisca sotto la sua autorità (c.d. autorizzati) che abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso. Il Responsabile è tenuto a:

1) individuare per iscritto i soggetti autorizzati al trattamento dei dati personali (persone fisiche o gruppi omogenei);

2) impartire ai soggetti autorizzati al trattamento le istruzioni idonee alle attività da svolgere in accordo agli obblighi relativi al trattamento dei dati personali e alla politica di sicurezza dell'organizzazione;

3) assicurarsi che i soggetti autorizzati al trattamento dei dati personali, debitamente nominati, si siano impegnati a mantenere la confidenzialità o siano in ogni caso vincolati all'adempimento di obblighi legali di riservatezza, anche in relazione alle credenziali di accesso;

4) vigilare sull'operato dei soggetti autorizzati al trattamento in relazione all'accesso ai dati personali;

5) prevedere un piano di formazione destinato ai soggetti autorizzati al trattamento;

6) prescrivere necessarie cautele per assicurare che i soggetti autorizzati siano vincolati a precise regole relative all'utilizzo corretto dei dispositivi elettronici e strumenti di lavoro in uso;

7) assicurare che i soggetti autorizzati siano vincolati a precise regole relative al corretto utilizzo delle password, tra le quali l'assenza di riferimenti agevolmente riconducibili al soggetto autorizzato al trattamento;

8) redigere e mantenere aggiornato un elenco contenente gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare e quanto definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti al Titolare dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" e s.m.i..

3.3. GESTIONE DEGLI ASSET

Il Responsabile è tenuto ad implementare un processo finalizzato alla tenuta di un inventario delle risorse IT (hardware, software e rete) utilizzate per il trattamento dei dati personali. Tale processo prevede l'aggiornamento periodico e la mappatura dei ruoli aziendali che hanno accesso alle risorse IT utilizzate per il trattamento dei dati personali oggetto di nomina.

Nel processo di gestione degli asset deve essere previsto che, tenuto conto della natura dei dati personali trattati e del rischio analizzato, qualora sia ritenuto adeguato, il riutilizzo dei supporti di memorizzazione sia possibile solamente nel caso in cui le informazioni precedentemente contenute non siano recuperabili; in caso contrario, i supporti dovranno essere distrutti.

Il Responsabile, in considerazione del rischio analizzato, è tenuto a prevedere modalità di cancellazione sicura dei dati (es. wiping) e/o la sovrascrittura dei dispositivi contenenti dati personali; in alternativa, la loro distruzione fisica.

Il Responsabile garantisce che tutte le apparecchiature contenenti supporti di memorizzazione siano controllate per assicurare che ogni dato personale e i software concessi in licenza siano rimossi o sovrascritti in modo sicuro prima della dismissione o del riutilizzo dell'asset stesso.

3.4. CONTROLLO DEGLI ACCESSI LOGICI

Il Responsabile è tenuto ad adottare una politica e/o un processo di gestione degli accessi ai dati personali,

che preveda specifiche regole di controllo degli accessi basati sul principio del Least Privilege o del Need to Know, ovvero che assicurino che l'accesso ai dati sia riservato al solo personale che ne ha la reale necessità (ad esempio: restrizioni per ruoli specifici degli utenti).
Tale politica terrà conto, nell'ambito della gestione degli accessi ai sistemi che gestiscono dati personali, della definizione e della documentazione della segregazione dei ruoli e delle responsabilità (ad esempio: richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
In particolare, tale politica/processo dovrà prevedere che:

- l'accesso ai sistemi informatici avvenga esclusivamente da parte degli utenti abilitati solo attraverso modalità digitali di autenticazione sicura mediante l'impiego di credenziali di livello II;
- Tenendo conto del livello di rischio individuato, ove il Responsabile lo ritenesse adeguato, potrà essere previsto l'utilizzo di modalità di autenticazione forte quali, a titolo esemplificativo e non esaustivo, MFA e SSO;
- sia definita una password policy formalmente documentata che identifichi i principali requisiti di complessità e di aggiornamento delle password degli utenti, in accordo con le *best practice di settore*, le normative di riferimento e le politiche di gestione delle credenziali in vigore;
- il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri soggetti autorizzati al trattamento, neppure in tempi diversi;
- l'uso di account condivisi sia opportunamente limitato ai soli casi in cui strettamente necessario;
- sia operata la disattivazione delle credenziali di autenticazione del personale in caso venga a cessare la necessità di accesso da parte del soggetto autorizzato al trattamento o intervenga un'inattività prolungata e sia effettuata periodicamente l'attività di revisione delle utenze profilate volte a disabilitare gli account non attivi e/o non autorizzati;
- siano monitorati gli accessi degli amministratori di sistema agli archivi elettronici inclusi quelli accessibili da sistema operativo o data base management systems (*DBMS*);
- siano predisposte le necessarie procedure affinché, in caso di prolungata assenza o impedimento del soggetto autorizzato al trattamento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici. In tal caso, ove possibile, dovrà essere garantita la segretezza della custodia delle copie delle credenziali individuando preventivamente per iscritto i soggetti autorizzati a tale scopo.

Il Responsabile è tenuto a prevedere meccanismi e sistemi per la registrazione e memorizzazione dei log delle attività degli utenti e amministratori di sistema e ad implementare un processo strutturato finalizzato alla loro gestione. Tale processo dovrà prevedere meccanismi di protezione dei log al fine di evitare operazioni di manipolazione non autorizzate e meccanismi di segregazione/mascheramento dei dati degli audit log al fine di renderli disponibili agli utenti o ad Autorità Giudiziarie

3.5. CRITTOGRAFIA, PSEUDONIMIZZAZIONE E GESTIONE DELLE CHIAVI

Il Responsabile è tenuto ad adottare una policy formalmente definita che preveda, ove possibile e ritenuto adeguato in base al rischio individuato, soluzioni di crittografia e/o pseudonimizzazione sui dati personali. In particolare, il Responsabile applicherà le opportune tecniche di cifratura e crittografica rese disponibili dal DBMS in funzione della tipologia di dati trattati.

A titolo esemplificativo, la policy potrà prevedere qualora siano trattati dati di tipo particolare, che la memorizzazione di tali dati su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'Interessato, ovvero che la memorizzazione dei dati particolari sia cifrata o in alternativa che vi sia separazione tra i dati particolari e gli altri dati personali che possano permettere l'identificazione dell'Interessato.

Tale policy dovrà disciplinare la gestione delle chiavi di cifratura in modo che siano allocate su apparati che garantiscano i principi di integrità e affidabilità e che siano previsti meccanismi di conservazione sicura.
Tale policy dovrà prevedere, ove possibile e in base quanto ritenuto adeguato in relazione al rischio individuato, che i dati in uso e a riposo e i dati degli ambienti di produzione e pre-produzione siano protetti mediante meccanismi di crittografia sicura attraverso l'utilizzo di algoritmi standard, open source e validati (ad esempio AES-256).

3.6. SICUREZZA FISICA E AMBIENTALE

Il Responsabile è tenuto ad adottare una policy formalmente definita che preveda, ove possibile e ritenuto

adeguato in base al rischio individuato, la protezione del perimetro fisico dell'infrastruttura del sistema IT da accessi non autorizzati tramite misure quali, ad esempio:

- un sistema di rilevamento intrusioni o barriere fisiche;
- il monitoraggio degli accessi ai locali dell'organizzazione sia da parte del personale interno che dei visitatori (ad esempio tramite lettori badge identificativi);
- la registrazione (registro fisico o registrazione a traccia elettronica) di tutti gli accessi alle zone sicure (es. sala server).

Tale policy dovrà disciplinare la gestione della protezione della sala server mediante misure quali, ad esempio, un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS).

3.7. GESTONE DEGLI ASPETTI DI SICUREZZA NELLE IT OPERATIONS

In ambito di Change Management, il Responsabile è tenuto ad adottare un sistema di gestione della qualità conforme alle best practice e agli standard internazionali (a titolo di esempio: *ISO 9001:2015 Quality management systems — Requirements*) per la progettazione e sviluppo di prodotti software che preveda , ove possibile e ritenuto adeguato in base al rischio individuato, l'utilizzo di un ambiente dedicato allo sviluppo/test delle modifiche applicative, segregato da quello di produzione e non contenente dati reali. Alla luce di ciò i team di sviluppo e di gestione delle evoluzioni procedono in modo conforme alle procedure definite dal Titolare.

Ove l'utilizzo di dati fittizi non fosse tecnicamente consentito, la policy dovrà formalmente identificare le misure tecniche adeguate a limitare l'accesso ai dati personali presenti in ambiente di test al solo personale autorizzato. Inoltre, la policy dovrà prevedere due installazioni differenti del *sistema* per effettuare le modifiche evolutive e correttive e per gestire il sistema in produzione.

Il Responsabile è tenuto ad adottare e aggiornare le principali misure di sicurezza ritenute adeguate ai fini del rilevamento malware e/o virus (es. antivirus, firme di rilevamento, sessioni limitate, aggiornamenti critici di sicurezza).

Il Responsabile è tenuto ad adottare un processo di gestione delle vulnerabilità che preveda, ove richiesto, l'esecuzione periodica di test di vulnerabilità e/o di penetration test.
Ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, tale processo dovrà prevedere la valutazione degli eventuali impatti derivanti dall'aggiornamento e, ove possibile e ritenuto adeguato in base al rischio individuato, il successivo l'aggiornamento, entro un congruo periodo di tempo, dei programmi utilizzati.

Il processo di gestione delle vulnerabilità deve prevedere l'installazione automatica delle patch di sicurezza sui sistemi per la risoluzione delle vulnerabilità rilevate. In caso di indisponibilità o tempi di distribuzione delle patch non compatibili con quelli previsti dall'organizzazione, il Responsabile è tenuto alla valutazione ed eventuale adozione di misure alternative.

3.8. BACK UP, BUSINESS CONTINUITY E DISASTER RECOVERY

Il Responsabile è tenuto a adottare una policy e processi formalmente definiti che prevedano l'esecuzione di copie di back-up delle informazioni e, ove possibile e ritenuto adeguato, del software e delle immagini dei sistemi. Tali procedure dovranno prevedere l'esecuzione di test periodici.

Il Responsabile mette in atto le misure di sicurezza adeguate affinché i supporti contenenti almeno una copia di backup non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

Il Responsabile è tenuto a prevedere un Piano di Continuità Operativa e un Piano di Disaster Recovery che prevedano, oltre che la definizione dei ruoli e delle responsabilità, anche la pianificazione di test periodici al fine di garantire la continuità delle operazioni indispensabili per l'erogazione del servizio e il ritorno alla normale operatività.

3.9. SICUREZZA DELLE COMUNICAZIONI

Il Responsabile è tenuto ad adottare misure di sicurezza adeguate in modo che il trasferimento dei dati

particolari in formato elettronico, avvenga attraverso “canali sicuri” o in maniera cifrata.

Il Responsabile è tenuto ad adottare adeguati meccanismi di protezione a livello di rete tra i quali, ad esempio, la configurazione sicura di protocolli e delle porte per lo svolgimento delle attività fondamentali, la protezione del traffico di rete, il monitoraggio del traffico nonché delle prestazioni del sistema al fine di rilevare le anomalie che potrebbero essere correlate a potenziali attacchi. Il Responsabile è tenuto a prevedere che i meccanismi di protezione a livello di rete adottati siano sottoposti ad una revisione periodica, in base al rischio individuato.
Il Responsabile è tenuto a garantire che l’accesso via internet sia limitato mediante l’utilizzo di misure tecniche adeguate (es. firewall, IPS, etc.) e ad installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo da aggiornare periodicamente ed in occasione di ogni versione disponibile dalla casa costruttrice.

3.10. SVILUPPO SICURO DEL SOFTWARE

Il Responsabile è tenuto ad adottare una policy formalmente definita che preveda, ove possibile e ritenuto adeguato in base al rischio individuato, che le interfacce applicative (API) siano progettate, sviluppate, implementate e testate in conformità con i principali standard del settore. Tali policy dovranno prevedere che le applicazioni siano sviluppate in accordo con metodologie di sviluppo sicuro dettate da enti riconosciuti a livello internazionale (e.g. OWASP), ivi compreso l’utilizzo di librerie ritenute sicure e opportune attività di analisi.

3.11. GESTIONE DEGLI INCIDENTI DI SICUREZZA E DATA BREACH

Il Responsabile è tenuto a redigere ed aggiornare periodicamente una procedura di gestione degli incidenti/violazioni di dati personali, che contempli un processo di analisi dei rischi e ove ritenuto applicabile, la notifica al Titolare e/o alle Autorità competenti, in conformità alla normativa privacy applicabile.
Il Responsabile, in ogni caso, venuto a conoscenza di una specifica violazione dei dati personali, sarà tenuto a comunicare al Titolare, ai sensi dell’art. 33, par. 2 GDPR, senza ingiustificato ritardo, le violazioni intervenute durante la vigenza della presente nomina, inoltrando la segnalazione ai punti di contatto indicati nel par. 10 del presente Atto. In ipotesi di intervenute violazioni dei dati personali, il Responsabile del trattamento collaborerà attivamente con il Titolare del trattamento per la corretta gestione della comunicazione delle violazioni summenzionate.
Il Responsabile predispone una lista contenente i contatti delle strutture organizzative coinvolte nella gestione degli incidenti di sicurezza, in modo da favorire il coordinamento in caso di incidente.
Il Responsabile definisce e applica opportune procedure per l’identificazione, la raccolta, l’acquisizione e la conservazione degli elementi che possono essere impiegati come evidenze nella gestione degli incidenti di sicurezza. Rilevato un incidente, il Responsabile garantisce di utilizzare una classificazione che sia in conformità alle normative.

4. OBBLIGHI INERENTI AI TRATTAMENTI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI

In merito al trattamento dei dati personali con strumenti diversi da quelli elettronici, il Responsabile è tenuto a predisporre un archivio per gli atti ed i documenti con dati personali individuando per iscritto i soggetti autorizzati al trattamento con i relativi profili di accesso ai dati ed ai documenti.
Devono essere definite le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio, un registro e degli armadi separati e chiusi).

Il trattamento di dati particolari dovrà infine prevedere l’utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi.

5. OBBLIGHI INERENTI LA DIFFUSIONE E IL TRASFERIMENTO DI DATI PERSONALI

È fatto assoluto divieto al Responsabile designato della diffusione dei dati, della comunicazione non autorizzata a terzi e più in generale è fatto divieto di effettuare trattamenti non finalizzati all’esecuzione delle attività affidate, salvo a fronte di specifica autorizzazione da parte del Titolare.

È fatto divieto al Responsabile di trasferire i dati personali trattati verso paesi non appartenenti all’Unione Europea se non previa autorizzazione scritta del Titolare e in conformità alle istruzioni ricevute nonché alle

condizioni di cui agli articoli 45, 46, 47, 48 e 49 del Regolamento che legittimano tale trasferimento e in particolare a condizione che il Responsabile garantisca, sotto la propria esclusiva responsabilità, che nel Paese terzo importatore dei dati il livello di protezione di questi ultimi sia “sostanzialmente equivalente” a quello in vigore presso il SEE e che il diritto del Paese terzo non interferisca con le misure adottate in modo tale da impedirne l’efficacia.