ACCORDO PER LA NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 PAR. 3 DEL REGOLAMENTO EUROPEO SULLA PRIVACY (N. 679 DEL 27 APRILE 2016 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO) a valere anche quale "**istruzione documentata**" di cui al medesimo articolo.

La Società della salute Fiorentina Sud-Est (di seguito SDS Fiorentina Sud Est), con sede legale in Bagno a Ripoli (Fi), Piazza della Vittoria n. 1 CAP 50012 nella persona legale rappresentante, Dr. Francesco Casini, domiciliato per la carica presso la suddetta società;

E

L'Ente di supporto tecnico amministrativo regionale (di seguito Estar), con sede legale in Firenze, Via di San Salvi n. 12 Pal. 14, di seguito denominato "Responsabile del Trattamento", rappresentato dal Direttore Generale, Dr. Massimo Braganti, domiciliato per la carica presso il suddetto Ente;

Premesso che:

- il Regolamento Europeo n. 2016/679 (di seguito "RGPD"), volto a tutelare le persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati, all'art. 4 par.1, punto 8 definisce il Responsabile del trattamento (di seguito Responsabile) come "la persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento";

- il Titolare del trattamento (di seguito Titolare) deve individuare il Responsabile tra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo di sicurezza, e che garantisca la tutela dei diritti dell'interessato;

- l'art. 28, par. 3, del RGPD, prevede che i trattamenti effettuati per conto del Titolare del trattamento (SDS Fiorentina Sud-Est) da parte di un Responsabile siano regolati da un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la natura e la finalità, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare;

- ai fini del rispetto della normativa, ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie attività;

- il Responsabile deve procedere al trattamento secondo le istruzioni impartite dal Titolare per iscritto con il presente atto, nell'allegato 1 e con eventuali accordi successivi;

- il presente atto è sottoscritto secondo quanto disposto dal RGPD e dal Codice Privacy, e nelle more della messa a disposizione da parte dell'Autorità di controllo degli schemi tipo di cui all'art. 28 par. 8 del RGPD;

- è intenzione del Titolare consentire l'accesso sia al Responsabile, che alle persone da questi autorizzate al trattamento, per i soli dati personali la cui conoscenza è necessaria per adempiere ai compiti loro attribuiti;

- il presente atto si applica al trattamento dei dati personali svolti dal Responsabile per conto della SDS Fiorentina Sud-Est, quale Titolare ai sensi della convenzione e definisce gli obblighi delle parti in materia di tutela dei dati personali;

- con Convenzione del 05/09/2022 si è proceduto ad affidare ad **ESTAR,** il servizio di "GESTIONE ASPETTI GIURIDICO-ECONOMICI RIGUARDANTI IL PERSONALE DIPENDENTE DELLA SOCIETA' DELLA SALUTE";

- ESTAR è in possesso dei necessari requisiti di conoscenza specialistica, affidabilità e risorse tali da fornire sufficienti garanzie per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa vigente e garantisca la tutela dei diritti dell'interessato;

si conviene e si stipula quanto segue:

ART.1

Oggetto, natura, finalità e durata del trattamento

1. Le premesse costituiscono parte integrante e sostanziale dell'accordo.
2. SDS Fiorentina Sud-Est quale Titolare a cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, in persona del suo legale rappresentante nomina ESTAR quale Responsabile dei trattamenti dei dati personali effettuati in relazione al servizio di cui in premessa.
3. I trattamenti dei dati personali per i quali Estar viene nominato Responsabile sono quelli afferenti l'adempimento della convenzione.
4. Il Responsabile provvederà al trattamento dei dati con logiche e modalità strettamente ed esclusivamente correlate alle finalità di diligente e regolare esecuzione del contratto, per il tempo strettamente necessario per il perseguimento delle finalità connesse, garantendo il pieno rispetto delle istruzioni ricevute, contenute nel presente accordo e nell'allegato 1 al presente atto.
5. Il Responsabile tratta i dati personali nella misura necessaria a fornire i servizi di cui al presente accordo.
6. Qualora sorgesse la necessità di trattamenti sui dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Responsabile dovrà informare preventivamente il Titolare.
7. I dati e le attività affidate al Responsabile del trattamento troveranno esecuzione esclusivamente nelle banche dati esistenti presso le infrastrutture del Titolare, o quelle espressamente individuate dalla convenzione. L'utilizzo di ulteriori supporti cartacei o digitali, potranno essere contemplati a patto che gli strumenti siano adeguatamente individuati ed inventariati dal Responsabile e sistematicamente comunicati al Titolare per sua approvazione. I dati personali dovranno essere contenuti in un archivio o destinati a figurarvi.
8. La presente nomina sarà efficace per tutta la durata del rapporto del Responsabile con il Titolare e dovrà intendersi automaticamente revocata in caso di cessazione dello stesso.

ART. 2

Tipologie di dati personali e categorie di interessati

1. Il trattamento potrà avere ad oggetto, a titolo esemplificativo:

- dati comuni (cognome e nome, residenza, domicilio, nascita, identificativo on line come username, password, customer ID, etc);
- situazione finanziaria, economica, patrimoniale e fiscale;
- dati relativi al rendimento professionale;
- categorie particolari di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose e filosofiche, o l'appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- dati giudiziari relativi a condanne o pendenze giudiziarie;
- dati relativi all'attività professionale svolta;
- dati relativi a titoli di studio dell'interessato.

2. I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente atto giuridico possono essere a titolo esemplificativo e non esaustivo:

- dipendenti e collaboratori della SDS Fiorentina Sud-Est;
- terzi autorizzati a qualunque titolo dal Titolare;
- controparti contrattuali del Titolare;
- in generale terze parti rispetto alle quali la SDS Fiorentina Sud-Est agisce come Titolare del trattamento dei dati personali;
- altro (specificare) _____

3. Resta inteso che il suddetto trattamento è consentito per le sole finalità inerenti la convenzione e si esclude quindi il riutilizzo delle informazioni per scopi diversi da quelli per i quali esse siano state originariamente raccolte.

ART. 3

Obblighi del Responsabile e modalità del trattamento

1. Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta. Il presente atto giuridico e la convenzione

costituiscono la totalità delle istruzioni del Titolare per il trattamento dei dati personali da parte del Responsabile.

2. Il Responsabile si impegna ad informare il Titolare laddove, a suo ragionevole giudizio, un'istruzione violi le disposizioni del RGPD o del Codice privacy, fermo restando che il Responsabile non è tenuto ad effettuare alcuna valutazione preventiva o successiva, circa la legittimità delle istruzioni ricevute dal Titolare. A tal proposito il Responsabile ha l'obbligo di inviare i rilievi, motivandoli dettagliatamente al seguente recapito del Titolare segreteria@pec.sds.firenze.it. In nessun caso il Responsabile è tenuto a conformarsi ad istruzioni del Titolare che siano in contrasto con la legge applicabile, e in particolare con il Codice Privacy o il RGPD.
3. Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nel contratto e nel presente atto giuridico deve essere fornita dal Titolare al Responsabile per iscritto e diviene efficace solo a seguito di ricezione da parte del Titolare della conferma scritta del Responsabile.
4. Il Responsabile, ai sensi dell'art. 28 par. 3 lett. a del RGPD, puo' trattare i dati personali del Titolare non solo alle condizioni di legittimità di quest'ultimo, ma anche se la legge applicabile cui è soggetto lo stabilisce. In tal caso il Responsabile informa il Titolare di tale obbligo giuridico prima del trattamento a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
5. Il Responsabile è tenuto a:

- organizzare, gestire e supervisionare tutte le operazioni di trattamento di competenza attenendosi ai principi generali e alle disposizioni della vigente normativa in materia di protezione dei dati personali, ovvero, assicurare che i dati personali oggetto del trattamento siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi; a tale riguardo, l'utilizzazione di dati personali e di dati identificativi dovrà essere ridotta al minimo, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi, ovvero adottando modalità che permettano di identificare gli interessati solo in caso di necessità;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità del trattamento;

- garantire il pieno rispetto delle istruzioni ricevute;

- tenere il registro delle attività di trattamento, ex art. 30 par. 2 del RGPD;
- conservare e custodire con diligenza, prudenza e perizia, i dati personali oggetto del trattamento;
- restituire al Titolare (oppure cancellare), in caso di cessazione del rapporto in essere o in qualsiasi momento il Titolare ne faccia richiesta, l'eventuale documentazione, su qualsiasi supporto, relativa a qualsiasi dato personale di cui sia entrato in possesso, senza che alcun dato possa essere direttamente o indirettamente detenuto;
- non vantare alcun diritto sui dati e sui materiali presi in visione;
- mantenere riservati, non comunicare e diffondere a terzi i dati personali e le informazioni di cui è venuto a conoscenza per effetto del trattamento;
- non utilizzare i dati personali e le informazioni, anche se in forma anonimizzata o pseudonimizzata, comprese le eventuali elaborazioni realizzate su disposizione del Titolare inerenti i trattamenti per finalità proprie o di terzi, anche successivamente alla cessazione del rapporto contrattuale in essere tra le parti.
- assistere il Titolare per quanto di competenza nel garantire il rispetto degli obblighi relativi alla sicurezza del trattamento, alla rilevazione di una violazione del trattamento, alla notifica di una violazione dei dati personali all'autorità di controllo, alla comunicazione di una violazione di dati personali all'interessato;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti ad esso riconosciuti dalla normativa vigente, supportando il Titolare nell'adempimento;
- attenersi alle specifiche disposizioni previste per il trasferimento di dati all'estero, qualora necessario, ed a non effettuare in alcun caso operazioni di diffusione dei dati stessi;
- su richiesta del Titolare assisterlo, nella misura in cui ciò sia ragionevolmente possibile, approntando le adeguate misure tecniche e organizzative, ai fini dell'adempimento da parte del Titolare al proprio obbligo di permettere ai terzi interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del RGPD;
- informare il Titolare, senza ingiustificato ritardo, laddove un terzo interessato eserciti uno dei diritti di cui al Codice Privacy e agli Artt. da 12 a 23 del RGPD, con particolare riferimento a, titolo esemplificativo, il diritto di accesso ai dati personali, il diritto di chiedere la rettifica e cancellazione (c.d. "diritto all'oblio") dei dati personali, il diritto di limitare il trattamento dei dati personali o di opporvisi, il diritto alla "portabilità" dei dati personali, il diritto di opporsi a una decisione basata unicamente sul trattamento automatizzato ai sensi dell'Art. 22 del RGPD;
- provvedere su richiesta del Titolare, o sulla base di provvedimenti dell'autorità di controllo o disposizioni dell'autorità giudiziaria, ad organizzare il blocco dei trattamenti soggetti a scadenza temporale (o la trasformazione in forma anonimizzata o pseudonimizzata) nei termini previsti dalla legge.

ART. 4

Soggetti autorizzati al trattamento

1. Il Responsabile, nell'ambito della propria struttura aziendale, provvederà ad individuare e designare le persone fisiche che devono compiere per suo conto operazioni del trattamento e/o attuare compiti relativi alla protezione e alla libera circolazione dei dati ai sensi dell'art. 2 quaterdecies del Codice Privacy.
2. Contestualmente alla designazione, il Responsabile si fa carico di fornire adeguate istruzioni scritte alle persone autorizzate al trattamento circa le modalità del trattamento, in ottemperanza a quanto disposto dalla legge e dal presente atto giuridico.
3. A titolo esemplificativo e non esaustivo, il Responsabile nel designare per iscritto le persone autorizzate al trattamento, dovrà prescrivere e verificare che:

   - abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
   - effettuino il trattamento dei dati personali in modo lecito e corretto, esclusivamente ai fini della prestazione dei servizi oggetto del rapporto contrattuale tra le parti;
   - trattino i dati personali unicamente per finalità inerenti i compiti loro assegnati;
   - non comunichino o diffondano i dati personali senza la preventiva autorizzazione del Titolare;
   - verifichino, in caso di interruzione anche temporanea del lavoro, che i dati personali trattati non siano accessibili a terzi non autorizzati;
   - custodiscano e mantengano strettamente riservate le credenziali di autenticazione;
   - rispettino le misure di sicurezza richieste dal Responsabile e/o dal Titolare.

4. Il Responsabile dovrà inoltre:

   - fornire specifica ed adeguata formazione agli autorizzati al trattamento dei dati oggetto del contratto ed impartendo loro, per iscritto, appropriate e complete istruzioni su come svolgere correttamente ed in modo lecito tale trattamento;
   - conservare idonea documentazione, da consegnare al Titolare a semplice richiesta, comprovante l'assolvimento degli obblighi di formazione e di conferimento istruzioni a tutti coloro che, a qualunque titolo, devono attuare compiti relativi alla protezione e alla circolazione dei dati;
   - garantire che i propri dipendenti e/o collaboratori che operano a vario titolo nell'ambito del rapporto in essere con il Titolare, siano dotati di esperienza, capacità e affidabilità con riferimento alla gestione dei sistemi informatici, nonché con riferimento alla normativa in materia di protezione dei dati personali, in particolare per quanto attiene alle misure di sicurezza previste.

5. Il Responsabile deve conformarsi al provvedimento generale del garante per la protezione dei dati personali del 27 novembre *2008 "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* , così come modificato dal Provvedimento del garante del 25 giugno 2009 *"Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento"*, ad ogni altro pertinente provvedimento dell'autorità, e alla procedura del Titolare PA 54/2018 "Gestione Amministratori di Sistema".

   Il Responsabile, ove previsto per le prestazioni contrattualizzate, si impegna in particolare a:

   - designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;
   - predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
   - comunicare al Titolare, su propria richiesta, l'elenco aggiornato degli amministratori di sistema;
   - verificare annualmente l'operato degli amministratori di sistema e comunicare, a richiesta del Titolare, le risultanze di tale verifica;
   - mantenere i file log previsti in conformità a quanto stabilito nel suddetto provvedimento, ove applicabile.

6. Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati alla riservatezza o abbiano un adeguato obbligo di riservatezza e che non usino, rivelino, divulghino in qualsiasi forma, anche per il periodo successivo al termine del rapporto di lavoro o di collaborazione, i dati personali conosciuti in occasione o a causa del rapporto di lavoro o di collaborazione con il Responsabile.

ART. 5

Sicurezza del trattamento

1. Il Responsabile si impegna ad adottare le misure di sicurezza richieste dall'art. 32 del RGPD.
2. In particolare, in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale a dati personali trattati, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile si impegna a mettere in atto le misure tecniche ed organizzative tra cui, se del caso, in particolare :
    - adottare un sistema di autenticazione informatica con credenziali di almeno otto caratteri;
    - permettere l'accesso solo agli utenti muniti di credenziali di autenticazione;
    - mantenere aggiornato l'ambito del trattamento consentito a detti autorizzati
    - adottare procedure di gestione delle credenziali di autenticazione, nonché di disattivazione delle stesse se non utilizzate da almeno sei mesi;
    - impartire istruzioni che regolino le modalità per assicurare la disponibilità dei dati personali in caso di prolungata assenza o impedimento dell'autorizzato;
    - proteggere gli strumenti elettronici e i dati personali rispetto a trattamenti illeciti e ad accessi non consentiti, adottando antivirus e software volti a prevenire la vulnerabilità di strumenti elettronici, da tenere costantemente aggiornati;
    - se previsto, adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati personali e dei sistemi, che prevedano il salvataggio dei dati personali con frequenza almeno settimanale;
    - impostare od adeguare i propri sistemi secondo i principi di privacy by design e privacy by default;
    - conservare i registri delle categorie di attività di trattamento svolte per il Titolare, mettendoli a disposizione del Titolare del trattamento su richiesta;
    - nominare ai sensi dell'art. 37 del RGPD un Responsabile della protezione dei dati (RPD) ove necessario.

3. Il Responsabile si riserva il diritto di apportare eventuali modifiche alle misure tecniche ed organizzative in considerazione del progresso e sviluppo tecnologico, fermo restando che tali modifiche non possono comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalla normativa vigente e nel presente accordo.
4. Il Responsabile deve fornire, su richiesta del Titolare, relazione scritta ad oggetto le misure di sicurezza adottate e quelle in progetto di adottare in relazione ai rischi per la protezione dei dati.

ART. 6

Nomina sub-responsabili del trattamento

1. Con il presente atto giuridico, il Titolare conferisce autorizzazione scritta generale al Responsabile a poter ricorrere ad eventuali ulteriori responsabili del trattamento (sub Responsabile/i), nella prestazione del servizio (subappalto; sub-affidamenti non soggetti a regime autorizzatorio, ecc.).
2. Il Responsabile, ai sensi di quanto previsto dall'art. 28 par. 4 del RGPD, può ricorrere ad altro soggetto per l'esecuzione di specifiche attività di trattamento per conto del Titolare assicurando che il suddetto soggetto offra garanzie sufficienti di affidabilità e riservatezza e metta in atto le misure tecniche ed organizzative adeguate cui è tenuto direttamente il Responsabile sulle attività interessate dal rapporto con il Titolare.
3. Il Responsabile disciplinerà i rapporti con il/i sub Responsabile/i con specifici contratti, o altri atti giuridici, a mezzo dei quali descriverà analiticamente i loro compiti, imponendo a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Titolare sul Responsabile.
4. L'elenco completo dei Sub-Responsabili del trattamento, cui il Responsabile intende affidare parte dell'attività contrattuale che prevede il trattamento di dati personali di cui alla convenzione in premessa, deve essere reso disponibile al Titolare prima della nomina. Il Titolare potrà quindi acconsentire esplicitamente la nomina come Sub-Responsabili del trattamento i soggetti tra quelli inclusi in tale elenco.
5. Qualora il/i sub Responsabile/i ometta/no di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile riconosce di conservare nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del/i Sub-Responsabile/i coinvolto/i, nonché si impegna a manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al Titolare dalla mancata osservanza di tali

obblighi e più in generale dalla violazione della normativa applicabile sulla tutela dei dati personali da parte del/i Sub-Responsabile/i.

6. Il Responsabile si impegna ad informare anticipatamente il Titolare, anche con mezzi elettronici (i.e. email), laddove intenda includere un nuovo Sub-Responsabile del trattamento nell'elenco reso disponibile o intenda sostituire un Sub-Responsabile del trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 1 (uno) mese dalla ricezione della comunicazione del Responsabile.
7. Qualora invece, il Titolare sollevi obiezioni, è tenuto a dettagliare al Responsabile le relative motivazioni. In tal caso, il Responsabile può a propria discrezione:

- proporre un altro Sub-Responsabile del trattamento in sostituzione del Sub-Responsabile del trattamento per il quale il Titolare abbia sollevato obiezioni; o
- adottare misure tese a superare le obiezioni del Titolare.

ART. 7

Trasferimenti verso paesi terzi o organizzazioni internazionali

1. Non essendo esplicitamente previsto nella convenzione, non è ammesso alcun trasferimento dei dati personali verso paesi terzi extraeuropei senza esplicito ulteriore consenso del Titolare.
2. In caso di autorizzazione da parte del Titolare, l'attività di trasferimento dei dati personali oggetto del trattamento dovrà essere comunque disciplinata da uno specifico accordo giuridico concluso tra le parti contenente le "Clausole contrattuali standard europee", ad integrazione di quanto definito dal presente documento. Nel caso in cui il Responsabile si avvalga di un Sub Responsabile anche le intese contrattuali intercorrenti tra dette parti dovranno essere conseguentemente integrate con la previsione delle "Clausole contrattuali standard europee", in modo che i medesimi obblighi incombenti sul Responsabile siano previsti anche in capo al Sub Responsabile che effettua il trasferimento di dati presso Paesi extra UE.
3. Il Responsabile dovrà comunque utilizzare modalità di trasferimento dei dati personali conformi a quanto previsto all'art. 44 e ss. del RGPD. In particolare il Responsabile dovrà garantire che adeguate misure tecniche ed organizzative siano approntate e documentate dai soggetti destinatari del trasferimento dei dati personali affinché il trattamento soddisfi i requisiti del RGPD e del Codice privacy novellato, sia assicurata la protezione degli

interessati, i trasferimenti dei dati possono essere tracciati, sia assicurata una adeguata procedura in caso di data breach, e la restituzione o completa distruzione dei dati alla fine del rapporto.

ART. 8

Attività di supporto al Titolare

1. Premesso che l'esercizio dei diritti di cui agli artt. da 12 a 23 del RGPD, da parte degli interessati sarà gestito direttamente dal Titolare, il Responsabile, si impegna, su richiesta del Titolare, ad assisterlo nella misura in cui ciò sia ragionevolmente possibile, ai fini dell'adempimento dell'obbligo di garantire agli interessati l'esercizio dei suddetti diritti.
2. In particolare, ove applicabile e in considerazione delle attività di trattamento affidategli, il Responsabile dovrà:

- permettere al Titolare di fornire agli interessati i loro dati personali in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, nonché di trasmettere i dati ad altro Titolare;
- permettere al Titolare di garantire in tutto o in parte i diritti di opposizioni e limitazione del trattamento.

3. Il Responsabile ha inoltre l'obbligo di:

- informare il Titolare, celermente e senza ingiustificato ritardo, di ogni comunicazione pervenuta dall'autorità di controllo o altre autorità;
- informare il Titolare, celermente e senza ingiustificato ritardo, di ogni attività di controllo o ispettiva nonché di ogni processo verbale e qualsiasi atto relativo a detta attività ispettiva e di controllo da parte dell'autorità di controllo o altre autorità;
- permettere al Titolare di acquisire ogni fatto o atto che ritenesse utile ai fini dell'osservanza delle norme e delle prassi in materia di protezione dei dati personali fornendo riscontro nei tempi indicati ai fini del rispetto degli obblighi di legge

    - informare immediatamente e senza ingiustificato ritardo il Titolare delle richieste e istanze pervenute dagli interessati, singoli o per il tramite di rappresentanti e associazioni;
    - informare il Titolare di ogni comunicazione indirizzata all'autorità di controllo o ad altre autorità, comprese controdeduzioni e scritti difensivi, preliminarmente al loro invio.

4. A richiesta del Titolare, il Responsabile dovrà garantire, per la parte di competenza, il rispetto degli obblighi relativi alla eventuale valutazione d'impatto sulla protezione dei dati personali nonché alla eventuale consultazione preventiva all'autorità di controllo ai sensi degli artt. 35 – 36 del RGPD.

ART. 9

Violazione dei dati personali (c.d. data - breach)

1. Tenendo conto della natura del trattamento come descritto nel contratto e nel presente atto giuridico, il Responsabile si impegna, su richiesta del Titolare, ad assisterlo nell'adempimento dei propri obblighi di cui agli artt. 33 e 34 del RGPD.
2. Il Responsabile deve comunicare al Titolare all'indirizzo pec segreteria@pec.sds.firenze.it , nel minor tempo possibile, e comunque non oltre le ventiquattro ore solari da quando ne abbia avuto conoscenza, qualsiasi distruzione, perdita, alterazione, divulgazione o accesso non autorizzato ai dati personali (data-breach), ivi incluse quelle che abbiano riguardato i propri sub responsabili, attivando comunque immediatamente le misure ritenute necessarie a interrompere la violazione e/o a mitigarne l'impatto.
3. In tale ipotesi, sarà compito del Responsabile fornire adeguata assistenza al Titolare comunicando almeno:

- una descrizione della natura della violazione dei dati personali e/o informazioni, comprese le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome ed i dati di contatto del Responsabile della protezione dei dati (RPD), o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione di dati personali e/o informazioni e le misure proposte o adottate dal Responsabile per porvi rimedio.

4. Quanto previsto al periodo che precede deve essere applicato anche qualora la violazione sia solo presunta o esista un sospetto pur in assenza di certezze.
5. Il Responsabile provvederà ad indicare al Titolare un riferimento di contatto per gestire queste eventualità.
6. Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, su richiesta, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad

arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi, al riguardo anche avvalendosi dell'operato di Sub Responsabili.

7. È fatto obbligo di mantenere l'assoluto riserbo sulle violazioni intercorse. Al riguardo tali notizie non dovranno essere in alcun modo diffuse in qualunque forma, anche mediante la loro messa a disposizione o consultazione. La comunicazione della violazione è ammessa solo tra il Titolare e/o altro soggetto da questo indicati e il Responsabile, fatte salve quelle comunicazioni richieste dalla legge o da autorità pubbliche.

ART.10

Cancellazione

1. Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile, questi a discrezione del Titolare e su richiesta di quest'ultimo sarà tenuto a:

- restituire al Titolare i dati personali oggetto del trattamento entro un termine ragionevole e al più tardi entro un mese, oppure
- provvedere alla loro integrale distruzione entro un termine ragionevole e al più tardi entro un mese salvo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc).

Resta salva l'ipotesi che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

2. In entrambi i casi il Responsabile provvederà a rilasciare al Titolare, dietro sua richiesta, apposita dichiarazione scritta contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità del Titolare. Il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.

ART. 11

Diritti di informazione e attività di verifica

1. Il Responsabile deve consentire al Titolare l'esercizio del potere di controllo ai sensi dell'art. 28 par. 3 lett. h del RGPD ed in tale contesto dovrà consentire al Titolare un'attività di

verifica (audit) realizzata dal Titolare stesso, al fine di accertare l'osservazione delle modalità di trattamento dei dati e il rispetto delle norme di legge.

2. Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un audit con ragionevole anticipo al più tardi 15 giorni prima della data fissata. Prima dell'audit le parti dovranno trovare un accordo circa l'oggetto, la tempistica e la durata dell'audit.
3. Il Titolare avrà facoltà di verificare, anche presso la sede del Responsabile, la conformità delle procedure adottate da quest'ultimo rispetto a quanto indicato nel presente accordo ovvero richiesto dalla normativa.
4. Il Titolare procederà attraverso interviste, esame della documentazione ed osservazioni sull'utilità e sulle condizioni operative al fine di raccogliere un numero di evidenze oggettive sufficiente alla determinazione della conformità ai requisiti prefissati. Il diritto rappresentato nel presente articolo si estende anche ad eventuali Sub-Responsabili.
5. Le ispezioni o gli audit potranno essere condotti da un revisore terzo indipendente incaricato dal Titolare, a condizione che detto revisore/auditor sia accettato dal Responsabile e sia vincolato agli obblighi di riservatezza.
6. Il Titolare dovrà fornire al Responsabile, entro un mese, una relazione scritta di natura confidenziale contenente un riepilogo dell'oggetto e dei risultati dell'audit. Il Responsabile ha il diritto di utilizzare tale relazione e le informazioni ivi contenute a propria discrezione.
7. Qualora il Titolare rilevasse comportamenti difformi a quanto prescritto dal presente atto, dalla normativa in materia, nonché dalle disposizioni contenute nei provvedimenti del Garante per la protezione dei dati personali, provvederà a darne comunicazione al Responsabile e, per il tramite di questo, ai suoi Sub–Responsabili, senza che ciò possa far venire meno l'autonomia dell'attività di impresa dei soggetti controllati ovvero possa essere qualificato come ingerenza nella loro attività.

ART. 12

Decorrenza dei termini

1. Il trattamento potrà essere svolto fino al termine della durata della convenzione, salve le successive operazioni, che dovranno essere completate entro sei mesi, di restituzione o cancellazione dei dati personali o dell'eventuale documentazione, su qualsiasi supporto, relativa a qualsiasi dato personale di cui è entrato in possesso, senza che alcun dato possa essere direttamente o indirettamente detenuto o comunque recuperabile dal Responsabile del trattamento.

2. Qualora il rapporto tra le parti venisse meno o perdesse efficacia per qualsiasi motivo o il servizio non fosse più erogato, anche il presente atto giuridico verrà automaticamente meno senza bisogno di comunicazioni o revoche ed il Responsabile, nonché gli eventuali Sub- Responsabili, non saranno più legittimati a trattare i dati personali di titolarità del Titolare.

ART. 13

Riservatezza

1. Il Responsabile si impegna a mantenere strettamente riservate e confidenziali ed a non utilizzare le informazioni riservate al di fuori degli scopi previsti dal presente accordo, né a rivelarle a soggetti non previsti dallo stesso, senza l'approvazione scritta del Titolare.

2. Il Responsabile garantisce che i soggetti incaricati ai fini dell'esecuzione dei servizi oggetto della convenzione, i quali potrebbero trattare i dati personali, si siano impegnati contrattualmente a mantenere la riservatezza dei dati o comunque sono soggetti a tale obbligo per legge.

3. Il Responsabile adotterà ogni misura necessaria a non divulgare o rendere in alcun modo disponibili le informazioni riservate del Titolare e/o degli interessati a terzi e sarà comunque ritenuto direttamente responsabile nei confronti del Titolare di ogni violazione da parte dei propri dipendenti e/o subfornitori degli obblighi di riservatezza di cui al presente articolo.

4. Le disposizioni del presente articolo non si applicano o cesseranno di applicarsi a quelle singole informazioni che il Responsabile possa dimostrare di essere:

- già divenute di pubblico dominio per ragioni diverse dall'inadempimento del Responsabile stesso;
- già note prima di averle ricevute dal Titolare;
- comunicate o divulgate in ottemperanza ad un ordine legittimo di qualsiasi autorità o in forza di un obbligo di legge.

5. Le informazioni riservate rivelate rimangono di proprietà del Titolare. A seguito di richiesta scritta dello stesso Titolare tali informazioni devono essere restituite o distrutte dal Responsabile.

ART. 14

Responsabilità

1. Il Responsabile tiene indenne e manlevato il Titolare da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante da o in connessione con una qualsiasi violazione da parte dello stesso delle disposizioni contenute nel presente accordo.

2. Il Responsabile risponde per il danno causato dal trattamento se non ha adempiuto agli obblighi del RGPD specificatamente diretti al Responsabile del trattamento, o ha agito in modo difforme o contrario rispetto alle istruzioni contenute nel presente atto.

3. Il Responsabile si obbliga a tenere manlevato ed indenne il Titolare da ogni responsabilità o danno, anche nei confronti di terzi, e da qualunque somma che il Responsabile del trattamento dovesse essere condannato a pagare, derivante direttamente o indirettamente da fatti attivi o omissivi ad esso imputabili esclusivamente, commessi anche dai dipendenti e/o collaboratori che operano a vario titolo come autorizzati al trattamento dei dati, ivi inclusi i danni derivanti dalla perdita, sottrazione, deterioramento e/o distruzione dei dati trattati.

4. Ai sensi dell'art. 82 par. 4 del RGPD, qualora il Titolare ed il Responsabile siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, sono responsabili in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo del danno.

5. Ai sensi dell'art. 82 par. 5 del RGPD, qualora il Titolare o il Responsabile abbia pagato l'intero ammontare del risarcimento del danno, sussiste il diritto di reclamare dal Titolare/Responsabile la parte del risarcimento corrispondente alla sua parte di responsabilità.

6. Il Responsabile del trattamento conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub Responsabile, qualora quest'ultimo ometta di adempiere agli obblighi in materia di protezione dei dati declinati nel RGPD o nel presente atto.

7. Ai sensi dell'art. 28 par. 10 del RGPD il Responsabile è reso edotto che, qualora violi il Regolamento, determinando autonomamente le finalità ed i mezzi del trattamento, verrà considerato Titolare del trattamento in questione.

   Rientra nella violazione del regolamento il disattendere le istruzioni ricevute dal Responsabile ai sensi dell'Art. 28 par. 4.

ART. 15

Modifiche ed integrazioni

1. Il Titolare si riserva, inoltre, ove ne ravvisasse la necessità, la facoltà di integrare ed adeguare, tempo per tempo, le istruzioni operative qui contenute, anche per conformarsi ad eventuali aggiornamenti normativi.

2. Di ogni modifica verrà data comunicazione al Responsabile a mezzo di raccomandata a/r o posta elettronica certificata. Trascorso il termine di trenta giorni, le variazioni si riterranno accettate dal Responsabile.

3. Per quanto non espressamente previsto nel presente accordo, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali.

ART. 16

Corrispettivo

1. In deroga a quanto disposto dall'art. 1709 cc, il presente incarico non prevede alcun compenso aggiuntivo a favore del Responsabile rispetto a quello già pattuito nel rapporto contrattuale tra le parti.
2. Con il presente atto giuridico si intende espressamente revocare e sostituire ogni altro accordo tra le parti inerente il trattamento dei dati personali.

Art. 17

Imposta di bollo

1. L'imposta di bollo è a carico del Responsabile e verrà assolta in maniera virtuale.
2. La presente convenzione sarà registrata in caso d'uso. In base all'articolo 15 comma 2 bis della legge 7 agosto 1990, n. 241 e ss.mm.ii. "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", il presente atto è sottoscritto dalle Parti con firma digitale, ai sensi dell'articolo 24 del decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii. "Codice dell'amministrazione digitale".

IL TITOLARE DEL TRATTAMENTO

Il Legale rappresentante

_____

IL RESPONSABILE DEL TRATTAMENTO

Il Legale rappresentante

_____

Società della Salute Fiorentina Sud-Est
Piazza della Vittoria 1 – 50012 Bagno a Ripoli (FI)
Via di Antella 58, Loc. Ponte a Niccheri – 50012 Bagno a Ripoli (FI)
sds.firenzesudest@uslcentro.toscana.it
C. F. 94297490487 – P. IVA 07179170480

ALLEGATO 1

Modalità ed istruzioni sul trattamento dei dati personali impartite dal Titolare del Trattamento nei confronti del Responsabile del trattamento, nell'ambito della presente nomina.

***

Il Responsabile del trattamento (di seguito "Responsabile") individuato è tenuto ad effettuare i trattamenti dei dati nel rispetto di quanto disposto dalla normativa sulla protezione dei dati personali, 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 a trattare i dati personali nel rispetto dei principi di necessità, pertinenza e non eccedenza, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza e la completezza dei dati e conservando gli stessi in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello occorrente alle finalità per i quali sono stati raccolti e trattati, e provvedendo, quando necessario, alla loro rettifica e aggiornamento.

Il Responsabile è tenuto ad iniziare eventuali nuovi trattamenti solo in seguito a richiesta da parte del Titolare del trattamento (di seguito "Titolare").

In caso di revoca della designazione a Responsabile, o di cessazione di un trattamento, 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 il Responsabile, prescriva la conservazione dei dati personali. In particolare, deve assicurare in ogni momento che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti, ai documenti contrattuali ed alle specifiche dei Servizi definiti dal Titolare. Le misure di sicurezza adottate dovranno, in ogni situazione, uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.

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 del RGPD, senza ingiustificato ritardo, tali violazioni, eventualmente intervenute durante la vigenza della presente nomina, secondo le modalità e procedure definite nell'atto di nomina. In ipotesi di intervenute violazioni dei dati personali, il Responsabile collaborerà attivamente con il Titolare per la corretta gestione della comunicazione delle violazioni summenzionate.

Il Responsabile è tenuto, in relazione ai soggetti autorizzati al trattamento che agiscono sotto la sua autorità, ad istruire quest'ultimi al rispetto delle seguenti misure:

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;

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

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

5) assicurarsi che ad ogni soggetto autorizzato al trattamento sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo del soggetto autorizzato al trattamento, eventualmente associato a un codice identificativo o a una parola chiave;

6) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo del soggetto autorizzato al trattamento;

7) assicurare che la parola chiave, quando è prevista dal sistema di autenticazione, sia composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili al soggetto autorizzato al trattamento e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi;

8) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri soggetti autorizzati al trattamento, neppure in tempi diversi;

9) assicurare che 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 per più di sei mesi;

10) predisporre 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 la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti autorizzati alla loro custodia;

11) prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo soggetto autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;

12) verificare, ad intervalli almeno annuali, le autorizzazioni in essere;

13) assicurare che nel caso di operatori telefonici, autorizzati al trattamento, questi nelle comunicazioni vocali scambiate durante lo svolgimento delle proprie attività si conformino alle disposizioni specificatamente emesse dal Responsabile per il rispetto dell'utenza e la riservatezza delle informazioni trattate;

14) redigere e mantenere aggiornato un elenco con 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 implementare le ulteriori misure di sicurezza, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" e ss.mm. ed ii.";

15) se previsto contrattualmente sulle macchine gestite dal Titolare, e comunque nelle macchine del Responsabile anche utilizzate per l'accesso da remoto e/o eventuali elaborazioni su macchine remote, installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo in accordo ai requisiti di legge da aggiornare comunque periodicamente;

16) provvedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un congruo periodo di tempo, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento;

17) se previsto contrattualmente sulle macchine gestite dal Titolare, e comunque sulle macchine del Responsabile che gestiscono dati oggetto della presente nomina, prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi.

In tema di sicurezza dei dati personali, ai sensi dell'art. 32 del RGPD, il Responsabile è tenuto a mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Nel valutare l'adeguato livello di sicurezza, si tiene 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.

Inoltre, per il trattamento di categorie particolari di dati personali (nel seguito, "dati particolari"), secondo la definizione dell'art. 9, par. 1 del RGPD, il Responsabile deve:

1) prevedere che 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. In questo ambito risulta necessario procedere a:

   a) emanare adeguate istruzioni di comportamento a tutti i soggetti autorizzati al trattamento;

   b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili, siano essi di tipo asportabile che presenti in aree di memoria interne al sistema operativo od in programmi, ove possano trovarsi dati particolari;

   c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni ai soggetti autorizzati al trattamento.

2) assicurare che la memorizzazione dei dati particolari su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'Interessato (anche attraverso processi di "pseudonimizzazione"), 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;

3) assicurare che il trasferimento dei dati particolari in formato elettronico, avvenga attraverso "canali sicuri" o in maniera cifrata.

In merito al trattamento dei dati personali con strumenti diversi da quelli elettronici, il Responsabile è tenuto a predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto i soggetti autorizzati 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.

E' fatto comunque 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.

Le operazioni di trattamento devono essere gestite dal Responsabile in aderenza alle attività svolte nell'ambito dei progetti assegnati e in considerazione di eventuali e successive modifiche alle operazioni e/o modalità di trattamento apportate dal Titolare.

Il Responsabile è chiamato ad assistere il Titolare nel garantire l'esercizio dei diritti eventualmente applicabili da parte degli interessati (Capo III del RGPD), nel rispetto dei termini di legge, adottando ogni soluzione organizzativa, logistica, tecnica e procedurale idonea ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali per l'esercizio degli stessi diritti.

Il Responsabile è tenuto a mettere a disposizione del Titolare tutte le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni, richieste dallo stesso Titolare o da altro soggetto da esso autorizzato, al fine di rilevare il rispetto degli obblighi previsti dalla normativa sulla protezione dei dati personali.

Il Responsabile, ai sensi dell'art. 30 par. 2 del RGPD e delle successive disposizioni dell'autorità di controllo, è tenuto a fornire al Titolare le informazioni necessarie alla compilazione del registro delle categorie di attività relative al trattamento. Qualora il Titolare intenda redigere la valutazione di impatto prevista dall'art. 35 del RGPD, il Responsabile sarà tenuto a fornire anche le ulteriori informazioni che si rendessero necessarie alla redazione del documento.

Il Responsabile, qualora in ottemperanza all'obbligo di legge, fosse tenuto ad individuare all'interno della propria organizzazione la figura del "Responsabile per la protezione dei dati personali (RPD)", quest'ultimo sarà tenuto a svolgere la propria attività in stretta collaborazione con il Responsabile.

Il Responsabile collaborerà attivamente con l'autorità di controllo, al fine di consentire a quest'ultima 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.

Misure tecniche ed organizzative

1. **Pseudonimizzazione e cifratura dei dati personali**

Il Responsabile nel servizio contrattualizzato non memorizza di norma particolari categorie particolari di dati personali fuori dalla gestione del software applicativo. Nel caso si verificasse la necessità di memorizzare categorie particolari di dati personali collegata alla attività di assistenza e manutenzione, il Responsabile separa i dati personali dai dati che tratta in modo tale che non sia possibile collegare il dato trattato a una persona identificata o identificabile senza avere informazioni aggiuntive, che sono archiviate dal Responsabile separatamente ed in modo sicuro. Il Responsabile, se del caso, provvede alla cifratura dei dati personali con chiavi simmetriche e asimmetriche.

2. **Riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi.**

a. Il Responsabile, se del caso, garantisce la riservatezza e integrità adottando le seguenti misure:

- controllo degli accessi: il Responsabile protegge i propri edifici con sistemi adeguati di controllo degli accessi. I diritti di accesso per le persone autorizzate sono concessi individualmente in base a criteri definiti. Ciò si applica anche a soggetti terzi che accedono agli edifici dell'azienda;
- controllo degli accessi al sistema: l'accesso ai sistemi di trattamento dei dati è concesso esclusivamente agli utenti autenticati sulla base di un concetto di autenticazione basato sui ruoli, che usa le seguenti misure: cifratura dei dati, assegnazione di password personalizzate (minimo 8 caratteri, scadenza regolare automatica), schede ID per i dipendenti con cifratura PKI, password complessa minimo 14 caratteri, salva schermo protetti da password in caso di inattività, sistemi di rilevamento di intrusioni e sistemi di prevenzione dalle intrusioni, antivirus aggiornati regolarmente e filtri spyware nella rete, sui PC individuali e sui dispositivi mobili;
- controllo degli accessi ai dati: l'accesso ai dati personali è concesso sulla base del concetto "autorizzazione fondata su ruoli". E' stato approntato un sistema di gestione degli utenti che associa il data base degli utenti con le rispettive autorizzazioni e che è disponibile centralmente in rete per essere recuperato su richiesta dei soggetti autorizzati al trattamento dei dati. Inoltre la cifratura dei dati previene accessi non autorizzati ai dati stessi;
- controllo della trasmissione dei dati: il Responsabile protegge i canali di comunicazione elettronica approntando reti chiuse e procedure di cifratura dei dati. Qualora abbia luogo un trasporto fisico, sono attuate procedure verificabili di trasporto che prevengono accessi non autorizzati ai dati o perdite dei dat. I trasferimenti dei dati sono disposti in osservanza delle normative sulla protezione dei dati.

b. Il Responsabile, se previsto contrattualmente, assicura disponibilità, resilienza ed affidabilità dei sistemi attraverso l'adozione delle seguenti misure:

- isolando i componenti IT e i componenti di rete critici, prevedendo un adeguato sistema di back up e di ridondanza, utilizzando sistemi di alimentazione ridondanti e verificando regolarmente sistemi e servizi. Le verifiche ed i sistemi live sono tenuti completamente separati.

3. **Disponibilità e accesso ai dati personali nell'eventualità di un incidente.**

Il Responsabile se previsto contrattualmente ripristinerà la disponibilità dei dati personali e l'accesso agli stessi nel caso di incidente fisico o tecnico, adottando le seguenti misure:

- il Responsabile conserva i dati personali in sistemi ridondati e secondo regole di sicurezza adeguate;
- database o banche dati di archivi di produzione e repliche o backup sono fisicamente conservati in luoghi diversi; almeno una copia dei dati è conservata fuori linea;
- è disponibile un esaustivo piano di emergenza, redatto per iscritto, che assicuri le procedure di ripristino nei tempi previsti in caso di incidente;
- le procedure ed i sistemi di emergenza sono rivisti regolarmente.

4. **Procedure di controllo per assicurare la sicurezza dei trattamenti dei dati personali.**

Il Responsabile, per i trattamenti effettuati al proprio interno, mantiene una procedura di controllo fondata su un approccio basato sul rischio, tenendo presente i cataloghi di protezione IT di base del Federal Office for Information Security (BSI) e i requisiti ISO/IEC 27001 per la revisione periodica, la valutazione e la verifica dell'efficacia delle misure tecniche e organizzative atte a garantire la sicurezza del trattamento. Ciò assicura la protezione delle informazioni rilevanti, delle applicazioni (compresi i metodi di verifica della qualità della sicurezza), degli ambienti operativi (ad esempio con il monitoraggio della rete dagli effetti dannosi) e l'implementazione tecnica dei concetti di protezione (ad esempio mediante analisi di vulnerabilità). Le misure protettive sono continuamente valutate e migliorate rilevando ed eliminando sistematicamente i punti deboli.

5. **Misure del personale.**

Il Responsabile istruisce per iscritto il personale che ha accesso a dati personali e organizza corsi di formazione al fine di garantire che i dati personali siano trattati solo in conformità alla legge applicabile, il presente atto giuridico, comprese le misure tecniche ed organizzative qui descritte.