ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI EX ART 28 DEL REGOLAMENTO UE 679/2016

tra

A.S.L. TARANTO, con sede in Viale Virgilio 31, 74100 Taranto CF e PI 02026690731 (di seguito anche la "Amministrazione" o il "Titolare"), in qualità di Titolare del trattamento ai sensi Regolamento UE 2016/679 (di seguito "Normativa in materia di Protezione dei Dati Personali" o "GDPR"), rappresentata legalmente dal Direttore Generale Avv. Stefano ROSSI

e

_____ P. IVA _____, con sede legale in_____, alla rappresentata legalmente dalla ..... , nel seguito per brevità definito anche "CAF Centro Assistenza Fiscale ";

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

1.1 Scopo delle presenti clausole contrattuali tipo (di seguito «clausole») è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

1.2 I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

1.3 Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

1.4 Gli allegati da I a IV costituiscono parte integrante delle clausole.

1.5 Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.

1.6 Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

Clausola 2 - Invariabilità delle clausole

2.1 Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

2.2 Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

3.1 Quando le presenti clausole utilizzano i termini definiti nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.

3.2 Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

3.3 Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

4.1 In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 — Clausola di adesione successiva

5.1 Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.

5.2 Una volta compilati e firmati gli allegati di cui alla clausola 5.1, l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.

5.3 L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II
OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento

6.1 I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7 - Obblighi delle parti

7.1. - Istruzioni

7.1.1. Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

7.1.2 Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. - Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. - Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. - Sicurezza del trattamento

7.4.1. Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da

ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

7.4.2 Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. - Dati sensibili (categorie particolari di dati)

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 (anche in linea con quanto disciplinato nel D.Lgs. 196/2003 e s.m.i. e dei provvedimenti specifici emanati dall'Autorità Garante per la protezione dei dati personali italiana).

7.6. - Documentazione e rispetto

7.6.1. Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

7.6.2 Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

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

7.6.4. Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

7.6.5. Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

7.7.1. Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno 30 giorni prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento al momento della sottoscrizione del presente contratto figura nell'allegato IV. Le parti tengono aggiornato tale allegato.

7.7.2. Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.

7.7.3. Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

7.7.4. Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

7.7.5. Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

7.8.1. Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

7.8.2. Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8 - Assistenza al titolare del trattamento

8.1. Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

8.2. Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle ai punti 8.1 e 8.2, il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

8.3. Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8.2, il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

- l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
- l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
- gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

8.4. Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali

9.1. In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.2. - Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

- la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.3. - Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.
d) Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III
DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione

10.1. Fatte salve le disposizioni del regolamento (UE) 2016/679 e/o del regolamento (UE) 2018/1725, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

10.2. Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

- il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità alla clausola 10.1 e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
- il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;
- il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole.

10.3. Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1.2, il titolare del trattamento insista sul rispetto delle istruzioni.

10.4 Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo

fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I
ELENCO DELLE PARTI

Titolare del trattamento:
ASL TARANTO
Indirizzo: Viale Virgilio 31, 74100 Taranto
Nome, qualifica e dati di contatto del referente: Avv. Stefano Rossi – Direttore Generale ASL Taranto

Responsabile/i del trattamento
CAF Centro Assistenza Fiscale
Indirizzo: …….
P.IVA : …….
Tel: - Fax:
P.E.C.: ……., e-mail ……
Nome, qualifica e dati di contatto del referente: …….

ALLEGATO II
DESCRIZIONE DEL TRATTAMENTO

Categorie di interessati i cui dati personali sono trattati

- In relazione ai servizi di Anagrafe Sanitaria Scelta e revoca del medico

Categorie di dati personali trattati

- In relazione ai servizi di Anagrafe Sanitaria Scelta e revoca del medico

Natura del trattamento

- I dati saranno trattati dal Responsabile mediante infrastrutture hardware e/o software, proprie e del Titolare per le attività ed i servizi dedicati.

Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

Il Responsabile è tenuto a trattare i dati esclusivamente per le finalità determinate, esplicite e legittime collegate ai servizi e alle attività sopra indicate

Per il perseguimento di tali finalità e per lo svolgimento delle attività sopra indicate, il Responsabile è tenuto a rispettare anche i provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali italiana, i principi di "privacy by design" e "privacy by default" nella realizzazione del servizio, nonché ogni altra misure di precauzione indicata dall'Autorità Garante per la Protezione dei Dati personali italiana e/o dal Comitato Europeo per la Protezione dei Dati.

Durata del trattamento

La presente nomina ha la medesima durata ed efficacia dell'Accordo in essere tra le Parti e, pertanto, cesserà al momento del completo adempimento o della cessazione della medesima, qualsiasi ne sia il motivo. Il trattamento, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i Dati Personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato. A seguito della cessazione del Trattamento affidato al Responsabile, nonché a seguito della cessazione del rapporto sottostante, qualunque ne sia la causa, il Responsabile sarà tenuto (a discrezione e su specifica indicazione del Titolare) a restituire in formato aperto al Titolare copia integrale dei Dati Personali trattati.

ALLEGATO III
MISURE TECNICHE E ORGANIZZATIVE, COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Il Responsabile, in considerazione della conoscenza maturata quale conseguenza dei progressi tecnici e tecnologici, della natura dei Dati Personali e delle caratteristiche delle operazioni di Trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, si obbliga a mettere in atto misure tecniche ed organizzative adeguate e dovrà assicurare che le misure di sicurezza progettate ed implementate siano in grado di eliminare o quantomeno ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi agli scopi di cui al presente Contratto.

In particolare, il Responsabile, anche per le attività di trattamento effettuate da ciascun dipendente e/o collaboratore esterno e ogni eventuale sub-fornitore (sub-responsabile) di cui si avvalga deve adottare tutte le necessarie misure di cui all'art. 32 del Regolamento Europeo n. 679/2016 – ove applicabili in ragione delle attività affidate - in modo da garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati, tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità Garante per la protezione dei dati personali italiana inerenti ai trattamenti svolti dal Responsabile. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito. In particolare, il Responsabile garantisce l'applicazione di specifiche misure di sicurezza come di seguito descritte:

- misure di pseudonimizzazione e cifratura dei dati personali
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- misure di identificazione e autorizzazione dell'utente (tra cui misure per controllare che sia consentito l'accesso ai propri sistemi informatici o di quelli della ASL tramite l'utilizzo di identificativi univoci per ciascun utente o amministratore di sistema interno, evitando identificativi condivisi tra più utenti, e attribuire a ciascun profilo di utenza i soli permessi di accesso ai sistemi necessari allo svolgimento delle rispettive mansioni operative: i permessi di accesso ai sistemi sui quali sono archiviati dati di titolarità della ASL devono essere rivisti su base annuale e comunque revocati qualora questi non siano più necessari)
- misure di protezione dei dati durante la trasmissione
- misure di protezione dei dati durante la conservazione
- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

- misure per garantire la registrazione degli eventi
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita
- misure di informatica interna e di gestione e governance della sicurezza informatica
- misure di certificazione/garanzia di processi e prodotti
- misure per garantire la minimizzazione dei dati
- misure per garantire la qualità dei dati
- misure per garantire la conservazione limitata dei dati
- misure per garantire la responsabilità
- misure per consentire la portabilità dei dati e garantire la cancellazione

Adottare, oltre alle misure di sicurezza sopra indicate, almeno le seguenti misure:

- procedure di autenticazione per utente e amministratore, nonché per tutelare l'accesso alle funzioni di amministratore; l'utilizzo delle utenze "Administrator", "root" e simili deve essere riservato alle sole emergenze e la distribuzione delle credenziali va effettuata in modo da assicurare l'imputabilità di chi ne fa uso;
- utilizzare credenziali amministrative di elevata robustezza e verificare periodicamente la riservatezza di dette credenziali, anche attraverso verifica presenza in data leak pubblici;
- impedire il riuso di password precedentemente utilizzate (password history);
- utilizzare e implementare funzionalità di "richiesta creazione o cambio della password al primo accesso", nonché di blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso;
- un sistema di gestione degli accessi per attività di supporto e manutenzione che operi sui principi del privilegio minimo e della necessità di comunicazione;
- garantire che le informazioni in transito tra le varie componenti del sistema siano adeguatamente protette e, se necessario, cifrate (ciò anche per le informazioni in transito tra il front-end e il back-end dell'applicazione) e implementare un tracciamento degli accessi ai servizi e ai dati, con monitoraggio continuo delle informazioni per rilevare in tempo reale eventuali attività sospette.
- utilizzare configurazioni sicure standard per la protezione dei sistemi operativi;
- definire una configurazione standard per server e altri tipi di sistemi utilizzati;
- sostituire le credenziali amministrative di default negli applicativi, framework o altro prodotto utilizzato per il trattamento di dati del Titolare;
- creare tanti utenti amministratori "nominali" quante sono le persone presenti nell'elenco ADS da fornire;
- registrare gli accessi degli utenti su un archivio (log) non cancellabile con il reset;
- verificare periodicamente la presenza delle copie di sicurezza (e fornire evidenza e garanzia del buon esito);
- assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante cifratura (provvedendo all'attivazione di strumenti di crittografia sulle copie di backup);
- adottare, sulle reti messe a disposizione dal Responsabile, i dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise).

Il Responsabile del trattamento, infine, deve prendere in considerazione, in termini di strumenti, prodotti, applicazioni o servizi forniti, i principi della protezione dei dati in base alla progettazione e per impostazione

predefinita (cc.dd. data protection by design e by default), tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità Garante per la protezione dei dati personali italiana inerenti ai trattamenti svolti e e le Linee Guida AGID su "La sicurezza nel procurement ICT".

Requisiti specifici per i servizi di gestione remota:

- i meccanismi di autenticazione devono essere basati su meccanismi di crittografia asimmetrica, a chiave pubblica; la lunghezza delle chiavi va impostata sulla base della criticità della comunicazione da cifrare (ad esempio 256 bit per le meno critiche, 512 bit per le più critiche). La gestione e distribuzione delle chiavi e dei certificati è a carico del Responsabile.
- Autorizzazione: sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni.
- Confidenzialità nella trasmissione dei dati: le comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'amministrazione devono essere cifrate.
- Fornire meccanismi che permettano di garantire l'integrità di quanto trasmesso (ad esempio meccanismi di hashing).
- Il Responsabile deve descrivere nel dettaglio le soluzioni tecniche utilizzate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza, …) per soddisfare i requisiti di sicurezza del Titolare.
- In fase di attivazione del servizio, il Responsabile deve concordare con il Titolare le modalità operative e le politiche di sicurezza, i livelli di gravità degli incidenti, le attività e le contromisure che dovranno essere svolte per contrastare le minacce.
- Il Responsabile dovrà attenersi alle politiche di sicurezza definite dalla committente, con particolare riferimento alla definizione di ruoli e utenze per l'accesso ai sistemi gestiti.
- In caso di necessità, da parte degli operatori, di accesso a Internet, il Responsabile deve utilizzare un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'amministrazione.
- In caso di rilevazione di un incidente di gravità elevata, il Responsabile deve dare immediata notifica, tramite canali concordati con il Titolare, dell'incidente rilevato e delle azioni da intraprendere, al Responsabile della Sicurezza indicato dal Titolare e agli organismi individuati dal legislatore a presidio della sicurezza cibernetica.
- Per ogni incidente di sicurezza, il Responsabile s'impegna a consegnare al Titolare, entro il giorno successivo, un report che descriva la tipologia di attacco subito, le vulnerabilità sfruttate, la sequenza temporale degli eventi e le contromisure adottate.
- Su richiesta del Titolare, il Responsabile deve consegnare i log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT. Tali log dovranno essere inviati al Titolare entro il giorno successivo a quello in cui è avvenuta la richiesta.
- Il Responsabile deve monitorare la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite. Entro il giorno successivo al rilascio dell'upgrade/patch/hotfix, lo stesso deve avviare una valutazione, da rilasciarsi entro un numero giorni da stabilirsi, propedeutica all'installazione delle stesse sui dispositivi di sicurezza, che ad esempio identifichi la possibilità di applicare la patch immediatamente, o la necessità di apportare MEV o integrazioni prima di procedere alle installazioni.

Attribuzione delle funzioni di amministratore di sistema

Il Responsabile deve assicurare la puntuale adozione delle misure di cui al Provvedimento dell'Autorità Garante per la protezione dei dati personali "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 e successive modifiche ed integrazioni. In particolare, il Responsabile deve:

- provvedere alla designazione degli amministratori di sistema in forma scritta su base individuale con elencazione analitica dell'ambito di operatività consentita in base al profilo di autorizzazione assegnata;
- stilare la lista degli amministratori di sistema e provvedere al relativo periodico aggiornamento. Tale lista dovrà includere gli estremi identificativi delle persone fisiche amministratori di sistema con l'elenco delle funzioni ad essi attribuite;
- fornire tempestivamente la lista aggiornata degli amministratori di sistema ogni qualvolta il Titolare ne faccia richiesta, anche tramite propri delegati e, in ogni caso, almeno una volta all'anno;
- consentire al Titolare la verifica almeno annuale sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i Trattamenti di Dati Personali;
- adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e degli archivi elettronici da parte degli amministratori di sistema. Le registrazioni devono:
  a. avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste;
  b. comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;
  c. essere conservate per un congruo periodo, comunque non inferiore a sei mesi e rese disponibili tempestivamente al Titolare, ogniqualvolta questi ne faccia richiesta, anche a mezzo di propri delegati.

Titolare del Trattamento Direttore Generale Avv. Stefano Rossi	Responsabile del Trattamento Centro Assistenza Fiscale