Azienda di Servizi alla Persona Golgi-Redaelli IT04737420150
Via Bartolomeo d'Alviano, n.78 - 20146, Milano (MI) - Italia
+39 02 7251 81 direzionegenerale@golgiredaelli.it

Registro dei trattamenti del titolare Azienda di Servizi alla Persona Golgi-Redaelli – ottobre 2026

Legale rappresentante

Nome e cognome	Email	Telefono fisso	Cellulare	PEC
Direttore Generale	direzionegenerale@golgiredaelli.it	-	-	direzione@pec.golgiredaelli.it

Data Protection Officer

Nome e cognome	Azienda	Telefono	Email	PEC
protezione dei dati responsabile	Azienda di Servizi alla Persona Golgi-Redaelli	02 72518215	privacy@golgiredaelli.it	privacy@pec.golgiredaelli.it

Dati del registro

Sedi	Tipo	# Tratt.	Codice revisione	Creato il	Modificato il	Esportato il	Autore
Sede legale (creata automaticamente), Istituto Geriatrico "P. Redaelli" MI, Istituto Geriatrico "P. Redaelli" VI, Istituto Geriatrico "C. Golgi" Documento approvato con Determinazione del Direttore Generale n. 293 del 02.11.2026	titolare	30	2026-Azi-PAR-033107-000584	22/09/2022	28/10/2026	28/10/2026 16:36	Cristina Callerio

Lista dei trattamenti (30 totale/i)

TRATTAMENTO	**Adempimenti relativi alla sicurezza sul lavoro**	
RISCHIO INIZIALE	**Alto (3)**	
RISCHIO RIDOTTO	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-041807-018
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Datore di Lavoro/Dirigente delegato
	Autorizzati al trattamento	Tutti gli autorizzati di Datore di Lavoro/Dirigente delegato
	Processo	Il trattamento concerne tutti i dati relativi alle attività connesse alla effettuazione degli adempimenti in materia di igiene e sicurezza sul lavoro. I dati sono oggetto di trattamento presso il datore di lavoro (o dirigente delegato) ed il medico competente, e presso le strutture organizzative di assegnazione, limitatamente al personale assegnato, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. • comunicazioni all'interessato: quando contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti dell'interessato o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovra' essere trasmesso, di regola, in plico chiuso, salva la necessita' di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto; • comunicazioni/trasmissioni interne: i documenti che contengono categorie particolari di dati, qualora debbano essere trasmessi ad altri uffici o funzioni della medesima struttura organizzativa in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, se non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine dovranno essere selezionate e impiegate modalita' di trasmissione della documentazione che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato.

	Elementi organigramma	Operazioni
OPERAZIONI	Datore di Lavoro/Dirigente delegato	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		N.B.: sono autorizzati/incaricati del trattamento tutti i dipendenti degli Uffici di Medicina del Lavoro Aziendale Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al MOP, nell'esecuzione del lavoro.
TITOLARI		Azienda di Servizi alla Persona Golgi-Redaelli

RESPONSABILI	**Ragione sociale**	**Attività**
	medico competente	-
	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	adempimento di specifici obblighi o svolgimento di compiti previsti dalla normativa in materia di prevenzione e sicurezza sul lavoro	obblighi di legge cui è soggetto il titolare del trattamento
	finalità di medicina del lavoro e valutazione della capacità lavorativa del dipendente	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Personale dipendente, personale inserito/da inserire a vario titolo presso l'Azienda (incarichi professionali, rapporti di consulenza e collaborazione, tirocinanti, volontariato e servizio civile) e personale appartenente ad altre organizzazioni, ma operante presso l'Azienda.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *soggetti deputati a: erogazione e liquidazione del trattamento di pensione; effettuazione di visite medico-collegiali o visite fiscali; effettuazione di accertamenti volti al riconoscimento di cause di servizio/equo indennizzo; vigilare sulla sicurezza sul lavoro; formazione del personale; fornire assicurazioni integrative * enti 12 che vantano crediti informativi *INAIL e autorità di P.S. per infortuni *enti coinvolti in comando di personale *organizzazioni sindacali e altri soggetti competenti per permessi e cariche sindacali *autorità giudiziaria). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio
	Destinatari	Medico Competente
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	

TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI		Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	l trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Amministratori, componenti di organismi, rappresentanti aziendali**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-025703-012
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	file system, carta, gestionale, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Mensilmente
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione generale
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione generale
	Processo	I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. La raccolta dei dati avviene principalmente presso i diretti interessati, anche tramite curriculum; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. Eventuali dati contenuti nei curricula, che non siano necessari per il perseguimento delle finalità del trattamento (procedimento nomine) non sono utilizzati, ma solo "conservati", in quanto inviati spontaneamente dagli interessati. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	Direzione generale	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di	

	trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	gestione dei dati degli amministratori aziendali e dei componenti di organismi diversi	adempimento di obblighi precontrattuali e contrattuali
	designazione, nomina e revoca di rappresentanti in commissioni, enti, istituti, uffici, organismi, associazioni etc.	Interesse pubblico rilevante
	erogazione di eventuali emolumenti e gestione di correlate problematiche fiscali e contributive	adempimento di obblighi precontrattuali e contrattuali
	accertamento di requisiti di onorabilità e	Interesse pubblico rilevante

	professionalità per le nomine presso persone giuridiche e soggetti pubblici e privati	
	registrazione sedute del CdI)	consenso - interesse pubblico rilevante
	partecipazione on line a sedute del CdI	consenso - interesse pubblico rilevante
CATEGORIE E TIPOLOGIE	**Interessati**	Amministratori, componenti di organismi, soggetti da nominare/nominati.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti

		agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Appalti di beni e servizi/di lavori: individuazione del contraente (dalla selezione alla stipula del contratto)**	
RISCHIO INIZIALE	**Medio (2)**	🟡
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-025419-007
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, con ausilio di strumenti elettronici, senza ausilio di strumenti elettronici,
	Numerosità degli interessati	Centinaia
	Frequenza del trattamento	Ogni ora
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Tecnico Patrimoniale, UOC Gestione Acquisti (Provveditorato-Economato)
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Tecnico Patrimoniale, Tutti gli autorizzati di UOC Gestione Acquisti (Provveditorato-Economato)
	Processo	In materia di instaurazione di rapporti commerciali/contrattuali/convenzionali il trattamento dei dati è finalizzato a instaurare il rapporto, sino alla stipula del contratto principale nonché di eventuali rinnovi e proroghe tecniche. I dati sono oggetto di trattamento presso le strutture organizzative rispettivamente competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Tecnico Patrimoniale	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

	UOC Gestione Acquisti (Provveditorato-Economato)	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI		Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**

	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
	Gestione albo fornitori	Consenso
	Instaurazione del rapporto contrattuale con fornitori e appaltatori, dalla partecipazione alle procedure di selezione sino alla stipula del contratto	adempimento di obblighi precontrattuali e contrattuali
CATEGORIE E TIPOLOGIE	**Interessati**	Fornitori, appaltatori, professionisti
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare,*Autorità Giudiziaria; *consulenti tecnici incaricati dall'Autorità Giudiziaria; *Autorità di vigilanza sui contratti; *Forze di Polizia; *Società assicuratrici; *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte *Agenzia delle entrate; *tutori, curatori e amministratori di sostegno). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei

		dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Appalti e contratti diversi: esecuzione del contratto**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-042819-027
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, con ausilio di strumenti elettronici, senza ausilio di strumenti elettronici
	Numerosità degli interessati	Centinaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione generale, UOC Comunicazione, URP e Marketing, UOS Avvocatura, UOC Direzione Operativa degli Istituti, UOC Affari Generali, UOC Bilancio, Programmazione Finanziaria e Contabilità, UOC Gestione e Sviluppo delle Risorse Umane, UOC Gestione Tecnico Patrimoniale, UOSD Servizi Diurni, UOSD Servizi specialistici, Servizio Infermieristico, Tecnico e della Riabilitazione aziendale, UOC Direzione Medica di Istituto - Milano, UOS Servizi Territoriali - Milano, UOS Demenze - Milano, UOS Cure Intermedie - Milano, UOS RSA e Hospice - Milano, UOC Direzione Medica di Istituto - Vimodrone, UOS Servizi Territoriali - Vimodrone, UOS Cure Intermedie - Vimodrone, UOC Direzione Medica di Istituto - Abbiategrasso, UOS Servizi Diurni - Abbiategrasso, UOS Demenze - Abbiategrasso, UOS Cure Intermedie - Abbiategrasso, Amministratore di Sistema, Servizio Accreditamento, Qualità e Risk management, Responsabile della Protezione dei Dati, Responsabile della Prevenzione della Corruzione e per la Trasparenza, UOC Gestione Acquisti (Provveditorato-Economato), Direttore del Dipartimento Sociosanitario, Direttore del Dipartimento Amministrativo, UOSD Gestione e Valorizzazione del Patrimonio, Datore di Lavoro/Dirigente delegato, Direzione Generale/Responsabile del Protocollo, Direttore esecuzione contratto/direttore lavori, UOC Gestione Operativa Milano, UOC Gestione Operativa Abbiategrasso-Vimodrone, UOS Sistemi Informativi aziendali, UOS Farmacia, UOC Disturbi cognitivi e Demenze Milano, UOS RSA Vimodrone, UOS RSA Abbiategrasso
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione generale , Tutti gli autorizzati di UOC Comunicazione, URP e Marketing, Tutti gli autorizzati di UOS Avvocatura , Tutti gli autorizzati di UOC Direzione Operativa degli Istituti, Tutti gli autorizzati di UOC Affari Generali , Tutti gli autorizzati di UOC Bilancio, Programmazione Finanziaria e Contabilità, Tutti gli autorizzati di UOC Gestione e Sviluppo delle Risorse Umane, Tutti gli autorizzati di UOC Gestione Tecnico Patrimoniale, Tutti gli autorizzati di UOSD Servizi Diurni, Tutti gli autorizzati di UOSD Servizi specialistici, Tutti gli autorizzati di Servizio Infermieristico, Tecnico e della Riabilitazione aziendale, Tutti gli autorizzati di UOC Direzione Medica di Istituto - Milano, Tutti gli autorizzati di UOS Servizi Territoriali - Milano, Tutti gli autorizzati di UOS Demenze - Milano, Tutti gli autorizzati di UOS Cure Intermedie - Milano, Tutti gli autorizzati di UOS RSA e Hospice - Milano, Tutti gli autorizzati di UOC Direzione Medica di Istituto - Vimodrone, Tutti gli autorizzati di UOS Servizi Territoriali - Vimodrone, Tutti gli autorizzati di UOS Cure Intermedie - Vimodrone, Tutti gli autorizzati di UOC Direzione Medica di Istituto - Abbiategrasso, Tutti gli autorizzati di UOS Servizi Diurni - Abbiategrasso, Tutti gli autorizzati di UOS Demenze - Abbiategrasso, Tutti gli autorizzati di UOS Cure Intermedie - Abbiategrasso, Tutti gli autorizzati di Amministratore di Sistema, Tutti gli autorizzati di Servizio Accreditamento, Qualità e Risk management, Tutti gli autorizzati di Responsabile della Protezione dei

		Dati, Tutti gli autorizzati di Responsabile della Prevenzione della Corruzione e per la Trasparenza , Tutti gli autorizzati di UOC Gestione Acquisti (Provveditorato-Economato), Tutti gli autorizzati di Direttore del Dipartimento Sociosanitario, Tutti gli autorizzati di Direttore del Dipartimento Amministrativo, Tutti gli autorizzati di UOSD Gestione e Valorizzazione del Patrimonio , Tutti gli autorizzati di Datore di Lavoro/Dirigente delegato, Tutti gli autorizzati di Direzione Generale/Responsabile del Protocollo, Tutti gli autorizzati di Direttore esecuzione contratto/direttore lavori, Tutti gli autorizzati di UOC Gestione Operativa Milano, Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone, Tutti gli autorizzati di UOS Sistemi Informativi aziendali, Tutti gli autorizzati di UOS Farmacia, Tutti gli autorizzati di UOC Disturbi cognitivi e Demenze Milano, Tutti gli autorizzati di UOS RSA Vimodrone, Tutti gli autorizzati di UOS RSA Abbiategrasso
	Processo	In materia di gestione di rapporti commerciali/contrattuali/convenzionali il trattamento dei dati è finalizzato a gestire il rapporto, sino alla conclusione dello stesso e all'espletamento degli incombenti connessi. I dati sono oggetto di trattamento presso le strutture organizzative rispettivamente competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
	Elementi organigramma	**Operazioni**
OPERAZIONI	**Direzione generale**	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Comunicazione, URP e Marketing	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOS Avvocatura	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Direzione Operativa degli Istituti	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

UOC Affari Generali	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Bilancio, Programmazione Finanziaria e Contabilità	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Gestione e Sviluppo delle Risorse Umane	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Gestione Tecnico Patrimoniale	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOSD Servizi Diurni	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOSD Servizi specialistici	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Servizio Infermieristico, Tecnico e della Riabilitazione aziendale	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Direzione Medica di Istituto - Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

UOS Servizi Territoriali - Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS Demenze - Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS Cure Intermedie - Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS RSA e Hospice - Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Direzione Medica di Istituto - Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS Servizi Territoriali - Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS Cure Intermedie - Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Direzione Medica di Istituto - Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

UOS Servizi Diurni - Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS Demenze - Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOS Cure Intermedie - Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Amministratore di Sistema	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Servizio Accreditamento, Qualità e Risk management	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Responsabile della Protezione dei Dati	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Responsabile della Prevenzione della Corruzione e per la Trasparenza	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Gestione Acquisti (Provveditorato-Economato)	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

Direttore del Dipartimento Sociosanitario	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Direttore del Dipartimento Amministrativo	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOSD Gestione e Valorizzazione del Patrimonio	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Datore di Lavoro/Dirigente delegato	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Direzione Generale/Responsabile del Protocollo	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
Direttore esecuzione contratto/direttore lavori	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Gestione Operativa Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

	UOS Sistemi Informativi aziendali	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOS Farmacia	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Disturbi cognitivi e Demenze Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOS RSA Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOS RSA Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		N.B.: sono autorizzati/incaricati del trattamento tutti i dipendenti degli Uffici appartenenti alla/e struttura/e di esecuzione del contratto/di direzione lavori Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: □ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; □ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; □ conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; □ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; □ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; □ qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; □ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; □ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; □ richiedere autorizzazione al

	Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
RESPONSABILI	**Ragione sociale**	**Attività**
	direttore esecuzione del contratto direttore lavori	esecuzione del contratto/della convenzione/di accordi diversi/direzione lavori
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**
	Gestione del rapporto contrattuale con fornitori e appaltatori, sino all'espletamento dell'incarico e degli incombenti connessi	adempimento di obblighi precontrattuali e contrattuali - Da specificare
	Gestione del contratto, collaudo, certificazione di regolare esecuzione, stati di avanzamento lavori e contabilità delle opere	adempimento di obblighi precontrattuali e contrattuali - Da specificare
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento - Da specificare
CATEGORIE E TIPOLOGIE	**Interessati**	Fornitori, appaltatori, professionisti, soggetti convenzionati o titolari di accordi diversi.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare,*Autorità Giudiziaria; *consulenti tecnici incaricati dall'Autorità Giudiziaria; *Autorità di vigilanza sui contratti; *Forze di Polizia; *Società assicuratrici; *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte *Agenzia delle entrate; *tutori, curatori e amministratori di sostegno). Nello svolgimento delle proprie

		funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Archivi e ricerca storica, registro dei benefattori, laboratori e iniziative culturali**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-025526-009
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale con e senza strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Affari Generali
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Affari Generali
	Processo	Il trattamento dei dati è finalizzato alla conservazione, ordinamento e comunicazione dei documenti conservati negli Archivi Storici dell'Azienda, nonché a fini storici, di studio, di ricerca e di documentazione, ai sensi delle vigenti disposizioni in materia archivistica. Inoltre, il trattamento dei dati – anche se prevalentemente riferiti a soggetti non più esistenti, e quindi "storicizzati" –, in particolare sotto il profilo della comunicazione e della diffusione, si rende necessario in occasione di laboratori, convegni e pubblicazione di testi e cataloghi, anche non connessi a manifestazioni ed eventi particolari. I dati sono, altresì, trattati per la gestione del registro dei benefattori e dei sostenitori, previsto per le ASP all'art. 27, c.1, lett. i) del Regolamento Regionale n. 11/2003, nonché per attività correlate a riconoscimenti ai benefattori e sostenitori medesimi (biografie, opuscoli, ritratti, etc.). I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia in modo centralizzato, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando, e avuto riguardo alle regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica vigenti nel tempo. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. Quando la raccolta dei dati avviene presso i diretti interessati, l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Affari Generali	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta,

		registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**

	conservazione, ordinamento e comunicazione dei documenti detenuti negli archivi storici degli enti pubblici	obblighi di legge cui è soggetto il titolare del trattamento
	ricerca storica	Interesse pubblico rilevante
	gestione degli archivi di deposito per conto delle strutture organizzative aziendali competenti mediante conservazione dei fascicoli di rispettivo interesse	obblighi di legge cui è soggetto il titolare del trattamento
	pubblicazioni di carattere storico e scientifico per l'ambito dei beni culturali	Interesse pubblico rilevante
	riconoscimenti gratulatori ai sostenitori e benefattori	consenso - interesse pubblico rilevante
	comunicazioni diverse relative all'attività ed ai contenuti degli archivi aziendali, a livello divulgativo, promozionale o statistico	Interesse pubblico rilevante
	organizzazione di laboratori, eventi e manifestazioni per l'ambito dei beni culturali	consenso - interesse pubblico rilevante
	gestione del registro dei benefattori e sostenitori	Interesse pubblico rilevante
CATEGORIE E TIPOLOGIE	**Interessati**	Soggetti i cui dati sono contenuti nei diversi archivi aziendali (storico, di deposito, corrente). Sostenitori, benefattori. Partecipanti a eventi, manifestazioni, progetti di carattere storico, artistico e culturale. Soggetti interessati a conoscere pubblicazioni, etc..
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
CONSERVAZIONE	**Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X -**	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.

	Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X	
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Attività di ricerca**	
RISCHIO INIZIALE	**Medio (2)**	
RISCHIO RIDOTTO	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-043934-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	Carta, file system, gestionale Con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Mensilmente
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOSD Servizi specialistici
	Autorizzati al trattamento	Tutti gli autorizzati di UOSD Servizi specialistici
	Processo	Il trattamento viene posto in essere per attività di studio e ricerca (connessi alle finalità istituzionali dell'Azienda e relativi allo sviluppo di conoscenze nelle materie di competenza e alla valutazione degli interventi effettuati, anche attraverso studi specifici). I dati vengono forniti dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati e le operazioni correlate alle attività di ricerca, specificati nei singoli progetti, qualora non sia possibile l'utilizzo di dati anonimi, sono trattati comunque in modo da non poter identificare gli interessati, a meno che l'abbinamento di tali dati identificativi al materiale di ricerca non sia temporaneo e essenziale per il risultato della ricerca, e motivato per iscritto nel progetto di ricerca. Per quanto e se applicabili alle attività condotte dalla Azienda in tal senso, si rimanda alle previsioni in materia di cui alle vigenti autorizzazioni generali del Garante. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOSD Servizi specialistici	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti

		con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**
	Scopi di ricerca scientifica	interesse pubblico rilevante.
	Stipula e gestione di sponsorizzazioni	Consenso

CATEGORIE E TIPOLOGIE	**Interessati**	Ospiti e utenti diversi degli Istituti geriatrici amministrati, parenti, familiari, care givers, amministratori di sostegno, curatori, tutori. Sponsor., ricercatori, tesisti e assimilabili
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X (per sponsor)
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X (per sponsor)
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *Aziende sanitarie; *Regioni e altre P.A. di riferimento; *Aziende ospedaliere, altre strutture di ricovero e cura e assimilabili; *enti privati; *Autorità giudiziaria; *Organi ispettivi; *soggetti esterni erogatori del servizio, anche in affidamento; *tutori, curatori e amministratori di sostegno; *soggetti facenti parte delle reti del FSE e della CRS, nonché degli erogatori di prestazioni per utenti cronici/fragili). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X (per sponsor)	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità

		dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Attività di tutela in sede amministrativa o giurisdizionale - assistenza e consulenza stragiudiziale**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-044330-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	file system, carta, gestionale Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Centinaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOS Avvocatura
	Autorizzati al trattamento	Tutti gli autorizzati di UOS Avvocatura
	Processo	I dati riguardano ogni fattispecie che possa dar luogo a un contenzioso e il loro trattamento può avvenire nell'ambito dell'intero procedimento di gestione dei contenziosi (in via stragiudiziale, in tutte le fasi e gradi di giudizio e nelle ipotesi in cui l'Azienda sia in veste di attore o convenuto, o comunque in qualsiasi caso e a qualunque titolo coinvolta) e nell'ambito di procedure non formalizzate in un contenzioso vero e proprio. I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia e presso eventuali altre strutture aziendali interessate, e secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOS Avvocatura	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il	

	trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	esercizio del diritto alla difesa in sede amministrativa e/o giudiziaria	Interesse pubblico rilevante
	attività di assistenza e consulenza stragiudiziale interna	Interesse pubblico rilevante
	accertamento della responsabilità civile, disciplinare e contabile	obblighi di legge cui è soggetto il titolare del trattamento

	esame dei ricorsi amministrativi	Interesse pubblico rilevante
	comparire in giudizio o partecipare alle procedure conciliative nei casi previsti dalla legge o dai CCNL	Interesse pubblico rilevante
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Soggetti coinvolti nei procedimenti giuridici o amministrativi; utenti, familiari, obbligati per legge; inquilini e affittuari stabili civili e fondi rustici; dipendenti, collaboratori a qualsiasi titolo, amministratori, partecipanti alle procedure ad evidenza pubblica, altri soggetti.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *soggetti controinteressati nell'istruttoria dei ricorsi amministrativi; *consulenti tecnici incaricati dall'Autorità Giudiziaria, collegi di conciliazione presso la Direzione provinciale del lavoro; *Autorità Giudiziaria; *Forze di Polizia; *Società assicuratrici (per la valutazione e copertura economica degli indennizzi per la responsabilità civile verso terzi); *incaricati di indagini difensive proprie e altrui, *consulenti della controparte; *eventuali Amministrazioni coinvolte; *Studi legali; *Cancellerie uffici giudiziari; *Agenzia delle Entrate e del Territorio). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale. Per le operazioni gestite dalla UOS Avvocatura e Gestione Legale si applicano le disposizioni di cui all'art. 4 dell'All. 1 della Delibera del Garante della Privacy n. 512 del 19.12.2018.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	

TERZI		
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Comunicazione istituzionale, marketing pubblico, fundraising e relazioni diverse con il pubblico**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-045427-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	file system, carta, app. gestionale, cloud, Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Settimanalmente
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. La raccolta dei dati avviene presso i diretti interessati o mediante consultazione di banche dati già costituite, prevalentemente a livello aziendale (banca dati ospiti, banca dati inquilini, banca dati fornitori, banca dati formatori, etc.). I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. L'informativa specifica agli interessati e l'acquisizione del consenso sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia (l'eventuale iscrizione del soggetto interessato ad un social network non implica un consenso generalizzato all'utilizzo dei dati per finalità diverse da quelle direttamente previste dal social network medesimo). Le attività per le quali i dati sono oggetto di trattamento e connesse alle finalità del medesimo vengono condotte anche facendo ricorso a flussi, metodi e strumenti telematici (sito web, social media, posta elettronica, contatti telefonici o via sms,...).
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il	

	trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: □ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; □ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; □ conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; □ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; □ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; □ qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; □ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; □ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; □ richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: □ utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); □ custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; □ modificare la password fornita al primo accesso, e poi ogni 3 mesi; □ adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; □ mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; □ non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), □ conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; □ curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; □ non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; □ evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet □ NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari □ NON utilizzare Google Drive o similari □ NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	I dati vengono, in particolare, trattati per: • Invio di comunicazioni istituzionali • Informazione destinata a soggetti esterni di riferimento, pubblici e privati • Relazioni e rapporti con cittadini, associazioni, istituzioni • Newsletter • Segnalazione e pubblicizzazione di iniziative • Inviti ad eventi e manifestazioni • Promozione	Consenso

	dell'immagine e dei servizi aziendali · Raccolta fondi e sostegni diversi · Campagne di marketing pubblico · Analisi di gradimento dei servizi esistenti // di richiesta di nuovi o diversi servizi Iniziative di marketing pubblico al fine precipuo di far conoscere i propri servizi e promuovere attività ed eventi connessi agli stessi, gestione e sviluppo di un sistema di relazioni per fidelizzare il rapporto con l'utenza e con i soggetti che abitualmente interagiscono con l'Azienda, innovazione ed ottimizzazione dei servizi avvalendosi di strumenti di customer satisfaction, ricorso a campagne di crowdfunding con il coinvolgimento di target mirati di riferimento	Consenso
CATEGORIE E TIPOLOGIE	**Interessati**	Soggetti potenzialmente interessati all'attività ed ai servizi aziendali, possibili sostenitori e simpatizzanti dell'ASP, utenti/ex utenti, familiari e care giver, soggetti inseriti in diverse banche dati già costituite presso l'Azienda o presso organizzazioni terze, soggetti corrispondenti a target mirati di riferimento per singola iniziativa.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali, nonché ad eventuali terzi gestori di banche dati assimilabili per ambiti di categoria e finalità, in particolare al fine di instaurare sinergie in ambito socio-sanitario-assistenziale anche con realtà afferenti al terzo settore o con qualifica di ONLUS. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	

TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI		Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Concessione di patrocinio**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-040853-023
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale con ausilio di strumenti elettronici senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Annualmente
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i

	dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	Concessione del patrocinio	Consenso
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	soggetti richiedenti il patrocinio
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di

		previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Dati giudiziari X	i dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e in ogni caso per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Contratti: gestione fidejussioni e garanzie, fatturazione, liquidazione e adempimenti contabili e tributari**	
RISCHIO INIZIALE	**Medio (2)**	🟡
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-043045-028
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	Carta, File system, Gestionale Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni ora
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Bilancio, Programmazione Finanziaria e Contabilità
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Bilancio, Programmazione Finanziaria e Contabilità
	Processo	In materia di instaurazione e gestione di rapporti commerciali/contrattuali/convenzionali il trattamento dei dati è finalizzato a instaurare e gestire il rapporto, sino alla conclusione dello stesso e all'espletamento degli incombenti connessi. I dati sono oggetto di trattamento presso le strutture organizzative rispettivamente competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Bilancio, Programmazione Finanziaria e Contabilità	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la	

	qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	Adempimenti contabili e tributari connessi alle posizioni contrattuali / adempimento di obblighi precontrattuali e contrattuali
CATEGORIE E TIPOLOGIE	**Interessati**: Soggetti titolari di contratti con l'ASP, e loro fiduciari.
	Categorie dati personali: Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X
	Tipologie dati personali: Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X

CONSERVAZIONE	**Categorie di destinatari**	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare,*Autorità Giudiziaria; *consulenti tecnici incaricati dall'Autorità Giudiziaria; *Autorità di vigilanza sui contratti; *Forze di Polizia; *Società assicuratrici; *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte *Agenzia delle entrate; *tutori, curatori e amministratori di sostegno). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Corsi e/o attività formative**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-044738-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni ora
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione e Sviluppo delle Risorse Umane
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione e Sviluppo delle Risorse Umane
	Processo	Il trattamento dei dati in occasione della formazione professionale concerne le informazioni relative alle richieste di partecipazione ai corsi e alla registrazione degli esiti degli stessi, ovvero in caso di offerta di sponsorizzazione. Il trattamento potrebbe riguardare dati sensibili inerenti lo stato di salute o l'origine etnica, o dati giudiziari, qualora i corsi fossero rivolti a determinate categorie di soggetti (es.: corsi per immigrati, per non vedenti, per ex carcerati). I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia in modo centralizzato, e presso le strutture organizzative di svolgimento dell'attività formativa, limitatamente ai partecipanti ai corsi, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione e Sviluppo delle Risorse Umane	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	n.b.: sono autorizzati/incaricati del trattamento anche *gli addetti alle segreterie della formazione presso gli Istituti, *gli addetti alla formazione di sicurezza. Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di	

un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.

TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

FINALITÀ, E BASI GIURIDICHE

Finalità	Base giuridica
Finalità di istruzione e formazione in ambito professionale	Interesse pubblico rilevante
Stipula e gestione di contratti di sponsorizzazione	Consenso
adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento

CATEGORIE E TIPOLOGIE	**Interessati**	Docenti, Sponsors, personale dipendente, personale inserito/da inserire a vario titolo presso l'Azienda, incarichi professionali, rapporti di consulenza e collaborazione, volontariato e servizio civile, soggetti esterni che partecipano ad iniziative formative aziendali
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso relativo a familiari dell'interessato - Dati giudiziari X (per sponsor)
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X - Dati giudiziari X (per sponsor)
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso relativo a familiari dell'interessato - Dati giudiziari X (per sponsor)	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.

IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Eredità, lasciti, legati e donazioni**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-040944-024
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system. con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Affari Generali
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Affari Generali
	Processo	Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Affari Generali	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle	

	istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	Accettazione e destinazione di eredità, lasciti, legati e donazioni / Consenso
CATEGORIE E TIPOLOGIE	**Interessati**: Testatori, eredi, cointeressati, donatori, notai, esecutori testamentari
	Categorie dati personali: Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X 56 - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Vita sessuale X - Dati giudiziari X
	Tipologie dati personali: Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X 56 - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Vita sessuale X - Dati giudiziari X

	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X 56 - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Vita sessuale X - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Gestione amministrativa, fatturazione, rendicontazioni, certificazioni degli ospiti**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-043827-032
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale. con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Milano
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Milano, Tutti gli autorizzati con mansione di Dirigente UOC
	Processo	Il trattamento viene posto in essere per l'effettuazione di tutte le attività correlate alla fornitura di assistenza in regime residenziale ad anziani e malati terminali, ad interventi per finalità socio-assistenziali, riabilitative, ambulatoriali e domiciliari, in regime residenziale o diurno, e ad altri servizi di natura diversa. Inoltre, il trattamento riguarda attività correlate a quelle di prevenzione, diagnosi, cura e riabilitazione, con riferimento all'erogazione di prestazioni specialistiche, di diagnostica strumentale e di laboratorio, e prestazioni accessorie di carattere alberghiero, ricreativo, assistenza religiosa. I dati vengono forniti, mediante presentazione di apposita istanza o di idonea prescrizione, dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per la gestione delle situazioni patologiche e per l'erogazione delle prestazioni socio-sanitarie agli interessati, nell'ambito delle finalità istituzionali dell'Azienda e in ottemperanza alla normativa regionale in materia. I dati etnici o relativi a particolari convinzioni religiose, filosofiche o di altro genere vengono trattati al fine di personalizzare le prestazioni e fornire un servizio maggiormente rispettoso delle diverse culture e tradizioni. Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o care givers dell'utente diretto, particolarmente per quanto riguarda la creazione del rapporto contrattuale fra il cliente e l'Azienda fin dal momento della richiesta del servizio, spesso non proposta dal diretto interessato. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del

		DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018.
	Elementi organigramma	**Operazioni**
OPERAZIONI	**UOC Gestione Operativa Milano**	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del

	lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione di ospiti solventi e dei soggetti assistiti dal SSN, e di assistenza domiciliare	Interesse pubblico rilevante
	assolvimento di adempimenti fiscali, tributari e contabili	obblighi di legge cui è soggetto il titolare del trattamento
	attività correlate all'applicazione della disciplina in materia di assistenza, integrazione sociale e diritti delle persone	adempimento di obblighi precontrattuali e contrattuali
	rilascio di certificazioni	obblighi di legge cui è soggetto il titolare del trattamento
	instaurazione, gestione, pianificazione e controllo dei rapporti con la Regione Lombardia, le Aziende Sanitarie Locali e le Aziende Ospedaliere, nonché con altri soggetti accreditati o convenzionati del Servizio Sanitario Nazionale e Regionale	adempimento di obblighi precontrattuali e contrattuali
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Ospiti e utenti diversi degli Istituti geriatrici amministrati, parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *Aziende sanitarie; *Regioni e altre P.A. di riferimento; *Aziende ospedaliere, altre strutture di ricovero e cura e assimilabili; *enti privati; *Autorità giudiziaria; *Organi ispettivi; *soggetti esterni erogatori del servizio, anche in affidamento; *tutori, curatori e amministratori di sostegno; *soggetti facenti parte delle reti del FSE e della CRS, nonché degli erogatori di prestazioni per utenti cronici/fragili). 20 Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.

	familiari dell'interessato X	
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Gestione assicurativa**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-040448-021
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	file system, carta, gestionale, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Centinaia
	Frequenza del trattamento	Settimanalmente
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOS Avvocatura
	Autorizzati al trattamento	Tutti gli autorizzati di UOS Avvocatura
	Processo	Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOS Avvocatura	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1.prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di

	autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche.In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	gestione dei rapporti assicurativi con riferimento a sinistri, danni, responsabilità verso terzi etc	adempimento di obblighi precontrattuali e contrattuali
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Utenti, familiari, obbligati per legge; inquilini e affittuari stabili civili e fondi rustici; dipendenti, collaboratori a qualsiasi titolo, tirocinanti, volontari; amministratori; partecipanti alle procedure di appalto; soggetti diversi danneggiati.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X

	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare *Società assicuratrici (per la valutazione e copertura economica degli indennizzi per la responsabilità civile verso terzi; *consulenti della controparte; *eventuali Amministrazioni coinvolte). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
CONSERVAZIONE	**Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X**	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale. Per le operazioni gestite dalla UOS Avvocatura e Gestione Legale si applicano le disposizioni di cui all'art. 4 dell'All. 1 della Delibera del Garante della Privacy n. 512 del 19.12.2018.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi

		trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Gestione dei beni immobili, locazioni, concessioni, acquisizioni e alienazioni**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-034645-014
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale - Con ausilio di strumenti elettronici X - Senza ausilio di strumenti elettronici X
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOSD Gestione e Valorizzazione del Patrimonio
	Autorizzati al trattamento	Tutti gli autorizzati di UOSD Gestione e Valorizzazione del Patrimonio
	Processo	In materia di instaurazione e gestione di rapporti contrattuali il trattamento dei dati è finalizzato a instaurare e gestire il rapporto, sino alla conclusione dello stesso e all'espletamento degli incombenti connessi. I dati sono oggetto di trattamento presso le strutture organizzative rispettivamente competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOSD Gestione e Valorizzazione del Patrimonio	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio,	

	al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	instaurazione e gestione del rapporto contrattuale con inquilini, affittuari, acquirenti, concessionari, di beni immobili di proprietà dell'Azienda (comprese manutenzioni ed altri aspetti tecnici)	adempimento di obblighi precontrattuali e contrattuali
	assolvimento di adempimenti fiscali, tributari e contabili	obblighi di legge cui è soggetto il titolare del trattamento
	tenuta di registri relativi a beni immobili	obblighi di legge cui è soggetto il titolare del trattamento

	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Inquilini, affittuari, acquirenti, concessionari, organismi di rappresentanza, enti e associazioni.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare,*Autorità Giudiziaria; *consulenti tecnici incaricati dall'Autorità Giudiziaria; *Autorità di vigilanza sui contratti; *Forze di Polizia; *Società assicuratrici; *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte *Agenzia delle entrate; *tutori, curatori e amministratori di sostegno). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali:

		identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Instaurazione di rapporti convenzionali e accordi diversi**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-034257-013
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, con ausilio di strumenti elettronici senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Affari Generali
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Affari Generali
	Processo	In materia di instaurazione di rapporti convenzionali il trattamento dei dati è finalizzato a instaurare il rapporto, sino alla conclusione dello stesso e all'espletamento degli incombenti connessi. I dati sono oggetto di trattamento presso le strutture organizzative rispettivamente competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Affari Generali	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle	

	istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: □ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; □ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; □ conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; □ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; □ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; □ qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; □ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; □ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; □ richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: □ utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); □ custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; □ modificare la password fornita al primo accesso, e poi ogni 3 mesi; □ adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; □ mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; □ non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), □ conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; □ curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; □ non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; □ evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet □ NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari □ NON utilizzare Google Drive o similari □ NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	Instaurazione di rapporti convenzionali, altri accordi ed intese con soggetti terzi — adempimento di obblighi precontrattuali e contrattuali
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione — obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**: Soggetti pubblici/privati e del Terzo Settore interessati al convenzionamento o alla stipula di altri accordi ed intese con l'ASP.
	Categorie dati personali: Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Dati giudiziari X
	Tipologie dati personali: Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Dati giudiziari X

	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare,*Autorità Giudiziaria; *consulenti tecnici incaricati dall'Autorità Giudiziaria; *Autorità di vigilanza sui contratti; *Forze di Polizia; *Società assicuratrici; *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte *Agenzia delle entrate; *tutori, curatori e amministratori di sostegno). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Instaurazione, gestione ed estinzione di rapporti di lavoro**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-042503-026
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni ora
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione e Sviluppo delle Risorse Umane
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione e Sviluppo delle Risorse Umane
	Processo	Il trattamento concerne tutti i dati relativi all'instaurazione e gestione del rapporto di lavoro presso l'Azienda, a partire dall'avvio delle procedure di accesso, che comporti o meno la costituzione di un rapporto di lavoro subordinato, nonché all'espletamento delle attività connesse alla gestione di volontari e addetti del servizio civile. Ha ad oggetto ogni attività e operazione concernente la gestione giuridica, economica, previdenziale, fiscale e pensionistica del personale e dei collaboratori, comprese le attività di formazione, le assicurazioni integrative, l'eventuale elaborazione diretta dei dati (su richiesta) per la presentazione assistita della dichiarazione dei redditi, agevolazioni economiche e contributi, adempimenti in materia di igiene e sicurezza sul lavoro e quant'altro sia necessario per la corretta gestione dei rapporti. I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia in modo centralizzato, e presso le strutture organizzative di assegnazione, limitatamente al personale assegnato, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Il trattamento viene eseguito anche applicando le seguenti cautele: • curriculum: il trattamento effettuato ai fini dell'instaurazione del rapporto di lavoro riguarda le sole informazioni strettamente pertinenti e limitate a quanto necessario a tali finalita', anche tenuto conto delle particolari mansioni e/o delle specificita' dei profili professionali richiesti; qualora nei curricula inviati dai candidati siano presenti dati non pertinenti rispetto alla finalita' perseguita i soggetti che effettuano la selezione devono astenersi dall'utilizzare tali informazioni; • dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico: il trattamento avviene esclusivamente in caso di fruizione di permessi in occasione di festivita' religiose o per le modalita' di erogazione dei servizi di mensa o, nei

		casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza; • dati che rivelano le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attivita' o di incarichi sindacali: il trattamento avviene esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali nonche' per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali; • partecipazione di dipendenti ad operazioni elettorali in qualita' di rappresentanti di lista: al fine del riconoscimento di benefici di legge, non vanno trattati nell'ambito della documentazione da presentare dati che rivelino le opinioni politiche (ad esempio, non deve essere richiesto il documento che designa il rappresentate di lista essendo allo scopo sufficiente la certificazione del presidente di seggio); • per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonche' in sede amministrativa o nelle procedure di arbitrato e di conciliazione: i dati vanno trattati esclusivamente per tali finalita' e per il periodo strettamente necessario al loro perseguimento; il trattamento di dati personali effettuato per finalita' di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose; • comunicazioni all'interessato: quando contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti dell'interessato o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovra' essere trasmesso, di regola, in plico chiuso, salva la necessita' di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto; • comunicazioni/trasmissioni interne: i documenti che contengono categorie particolari di dati, qualora debbano essere trasmessi ad altri uffici o funzioni della medesima struttura organizzativa in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, se non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine dovranno essere selezionate e impiegate modalita' di trasmissione della documentazione che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato; • quando per ragioni di organizzazione del lavoro, e nell'ambito della predisposizione di turni di servizio, si proceda a mettere a disposizione a soggetti diversi dall'interessato (ad esempio, altri colleghi) dati relativi a presenze ed assenze dal servizio, non si deve esplicitare, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilita' di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).
	Elementi organigramma	**Operazioni**
OPERAZIONI	**UOC Gestione e Sviluppo delle Risorse Umane**	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati	

	sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	Instaurazione, gestione ed estinzione dei rapporti di lavoro dipendente di qualunque tipo, anche a tempo parziale o temporaneo e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato, compreso adempimento di specifici obblighi o svolgimento di compiti previsti dalla normativa in materia di igiene e sicurezza sul lavoro	adempimento di obblighi precontrattuali e contrattuali
	erogazione di contributi economici/riconoscimento di agevolazioni al personale dipendente	adempimento di obblighi precontrattuali e contrattuali
	applicazione di normativa in materia di previdenza ed assistenza e in materia fiscale e sindacale	obblighi di legge cui è soggetto il titolare del trattamento
	tenuta della contabilità e corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori	adempimento di obblighi precontrattuali e contrattuali

salvaguardia dell'incolumità fisica del lavoratore o di terzi	obblighi di legge cui è soggetto il titolare del trattamento
attività di tutela e difesa di diritti in sede giudiziaria, amministrativa, di arbitrato o conciliazione	Interesse pubblico rilevante
garanzia delle pari opportunità	obblighi di legge cui è soggetto il titolare del trattamento
adempimento di obblighi assicurativi in materia di sicurezza o per danni a terzi	obblighi di legge cui è soggetto il titolare del trattamento
attività amministrative correlate all'applicazione della disciplina in materia di diritti delle persone handicappate	obblighi di legge cui è soggetto il titolare del trattamento
attività relative alla gestione di rapporti di servizio civile	Interesse pubblico rilevante
gestione dei registri del personale dipendente dall'Azienda e del personale appartenente ad altre organizzazioni, ma operante a vario titolo presso l'Azienda, previsto per le ASP all'art. 27, c.1, lett. h) e k) del Regolamento Regionale n. 11/2003, nonché degli elenchi dei curriculum e delle autocandidature	obblighi di legge cui è soggetto il titolare del trattamento
gestione dei curriculum e delle autocandidature	adempimento di obblighi precontrattuali e contrattuali
adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
In particolare, i dati vengono trattati, nell'ambito delle finalità di cui sopra, come di seguito sintetizzato: In fase preliminare alle assunzioni, per: • gestire concorsi, selezioni e procedure di assunzione diverse (mobilità, comando) • applicare la normativa in materia di collocamento obbligatorio e assumere personale, anche appartenente a categorie protette • garantire le pari opportunità • accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi – compresa l'esistenza di idoneità alla mansione -, anche in materia di tutela delle minoranze linguistiche • applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti • applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale Nel corso del rapporto di lavoro, per: • gestire gli istituti contrattuali, particolarmente in materia di assenza dal servizio per malattia, infortunio sul lavoro, inidoneità/inabilità, astensione obbligatoria, facoltativa o anticipata per maternità, congedi parentali • garantire le pari opportunità • accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi – compresa l'esistenza di idoneità alla mansione -, anche in materia	Quelle previste per il complesso delle finalità

		di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni • adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché obblighi retributivi, contributivi e fiscali o contabili relativamente al personale in servizio o in quiescenza, compresa la corresponsione di premi, agevolazioni e benefici assistenziali • adempiere specifici obblighi o compiti previsti dalla normativa in materia di medicina preventiva e del lavoro, igiene e sicurezza del lavoro o di sicurezza e salute della popolazione, nonché in materia sindacale (trattenuta della quota di iscrizione, permessi sindacali, esercizio dei diritti sindacali) • applicare la normativa in materia di previdenza ed assistenza, compresa quella integrativa, riguardo alla comunicazione di dati, anche in via telematica, agli istituti di patronato ed assistenza sociale, alle associazioni di categoria ed agli ordini professionali che abbiano ottenuto il consenso dell'interessato in relazione ai tipi di dati individuati specificamente • svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie• comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro; i dati sensibili sono oggetto di trattamento sia manuale sia automatizzato al fine di predisporre memorie che vengono presentate innanzi alle Commissioni di conciliazione competenti • applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti • applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale • svolgere l'attività di indagine e di ispezione presso soggetti pubblici • gestire i rapporti ai fini fiscali e previdenziali
CATEGORIE E TIPOLOGIE	**Interessati**	Personale dipendente, personale inserito/da inserire a vario titolo presso l'Azienda (incarichi professionali, rapporti di consulenza e collaborazione, tirocinanti, volontariato e servizio civile, candidati a concorsi e selezioni, presentatori di autocandidature) e personale appartenente ad altre organizzazioni, ma operante presso l'Azienda. Familiari e conviventi di lavoratori subordinati e di soggetti in rapporto di collaborazione o lavoro autonomo, per il rilascio di agevolazioni e permessi; terzi danneggiati nell'esercizio dell'attività lavorativa o professionale.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a

		partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Vita sessuale X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *soggetti deputati a: erogazione e liquidazione del trattamento di pensione; effettuazione di visite medico-collegiali o visite fiscali; effettuazione di accertamenti volti al riconoscimento di cause di servizio/equo indennizzo; vigilare sulla sicurezza sul lavoro; formazione del personale; fornire assicurazioni integrative * enti che vantano crediti informativi *INAIL e autorità di P.S. per infortuni *enti coinvolti in comando di personale *organizzazioni sindacali e altri soggetti competenti per permessi e cariche sindacali *autorità giudiziaria). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
CONSERVAZIONE	**Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X**	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne;

		assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Prestazioni accessorie ai servizi di cura e assistenza**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-043405-030
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Milano, UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Milano, Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	Il trattamento viene posto in essere per l'effettuazione di tutte le attività correlate alla fornitura di assistenza in regime residenziale ad anziani e malati terminali, ad interventi per finalità socio-assistenziali, riabilitative, ambulatoriali e domiciliari, in regime residenziale o diurno, e ad altri servizi di natura diversa. Inoltre, il trattamento riguarda attività correlate a quelle di prevenzione, diagnosi, cura e riabilitazione, con riferimento a prestazioni accessorie di carattere alberghiero, ricreativo, assistenza religiosa. I dati vengono forniti dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per l'erogazione delle prestazioni accessorie e complementari a quelle di assistenza e cura. I dati etnici o relativi a particolari convinzioni religiose, filosofiche o di altro genere vengono trattati al fine di personalizzare le prestazioni e fornire un servizio maggiormente rispettoso delle diverse culture e tradizioni. Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o care givers dell'utente diretto, particolarmente per quanto riguarda la creazione del rapporto contrattuale fra il cliente e l'Azienda fin dal momento della richiesta del servizio, spesso non proposta dal diretto interessato. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018.

	Elementi organigramma	Operazioni
OPERAZIONI	UOC Gestione Operativa Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X

ISTRUZIONI

Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e

	esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**
	Accettazione delle domande	adempimento di obblighi precontrattuali e contrattuali
	Stipula dei contratti con i clienti	adempimento di obblighi precontrattuali e contrattuali
	Gestione del rapporto contrattuale con l'utenza sotteso alla erogazione dei servizi e delle prestazioni e dei rapporti con altri enti e soggetti pubblici e privati	adempimento di obblighi precontrattuali e contrattuali
	Erogazione di prestazioni accessorie di carattere alberghiero, ricreativo, assistenza religiosa e spirituale	adempimento di obblighi precontrattuali e contrattuali
	Tenuta di registri relativi a beni mobili di proprietà degli ospiti	adempimento di obblighi precontrattuali e contrattuali
CATEGORIE E TIPOLOGIE	**Interessati**	Ospiti e utenti diversi degli Istituti geriatrici amministrati, parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *Aziende sanitarie; *Regioni e altre P.A. di riferimento; *Aziende ospedaliere, altre strutture di ricovero e cura e assimilabili; *enti privati; 16 *Autorità giudiziaria; *Organi ispettivi; *soggetti esterni erogatori del servizio, anche in affidamento; *tutori, curatori e amministratori di sostegno; *soggetti facenti parte delle reti del FSE e della CRS, nonché degli erogatori di prestazioni per utenti cronici/fragili). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database]

		database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Prestazioni ambulatoriali**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2023-Azi-070102-031
	Date	Creato il 09/03/2023, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	su carta, file sistem, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni ora
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOSD Servizi specialistici
	Autorizzati al trattamento	Tutti gli autorizzati di UOSD Servizi specialistici
	Processo	Il trattamento viene posto in essere per l'effettuazione di tutte le attività correlate alla fornitura di prestazioni ambulatoriali diverse su richiesta dell'interessato (anche con prenotazione online o per prestazioni di telemedicina). I dati vengono forniti, mediante presentazione di apposita istanza o di idonea prescrizione, dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per la gestione delle situazioni patologiche e per l'erogazione delle prestazioni agli interessati, nell'ambito delle finalità istituzionali dell'Azienda e in ottemperanza alla normativa regionale in materia. I dati etnici o relativi a particolari convinzioni religiose, filosofiche o di altro genere vengono trattati al fine di personalizzare le prestazioni e fornire un servizio maggiormente rispettoso delle diverse culture e tradizioni. Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o care givers dell'utente diretto, particolarmente per quanto riguarda la creazione del rapporto contrattuale fra il cliente e l'Azienda fin dal momento della richiesta del servizio, spesso non proposta dal diretto interessato. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018.
OPERAZIONI	**Elementi organigramma**	**Operazioni**

	UOSD Servizi specialistici - raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	NB.: sono autorizzati/incaricati del trattamento tutti i dipendenti degli ambulatori e dei CUP degli Istituti Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**
	interventi di prevenzione, diagnosi, cura e riabilitazione	Consenso
CATEGORIE E TIPOLOGIE	**Interessati**	utenti esterni, esercenti la patria potestà per minori
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali, nonché ad eventuali terzi gestori di banche dati assimilabili per ambiti di categoria e finalità, in particolare al fine di instaurare sinergie in ambito socio-sanitarioassistenziale. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità

		dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Prestazioni di assistenza, cura e tutela della salute**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-041723-026
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	Carta, gestionale, file system - Con auslio di strumenti elettronici - Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Direzione Medica di Istituto - Milano, UOC Direzione Medica di Istituto - Vimodrone, UOC Direzione Medica di Istituto - Abbiategrasso, UOC Disturbi cognitivi e Demenze Milano
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Direzione Medica di Istituto - Milano, Tutti gli autorizzati di UOC Direzione Medica di Istituto - Vimodrone, Tutti gli autorizzati di UOC Direzione Medica di Istituto - Abbiategrasso, Tutti gli autorizzati di UOC Disturbi cognitivi e Demenze Milano
	Processo	Il trattamento viene posto in essere per l'effettuazione di tutte le attività correlate alla fornitura di assistenza in regime residenziale ad anziani e malati terminali, ad interventi per finalità socio-assistenziali, riabilitative, ambulatoriali e domiciliari, in regime residenziale o diurno, e ad altri servizi di natura diversa. Inoltre, il trattamento riguarda attività correlate a quelle di prevenzione, diagnosi, cura e riabilitazione, con riferimento a prestazioni accessorie di carattere alberghiero, ricreativo, assistenza religiosa. I dati vengono forniti dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per l'erogazione delle prestazioni accessorie e complementari a quelle di assistenza e cura. I dati etnici o relativi a particolari convinzioni religiose, filosofiche o di altro genere vengono trattati al fine di personalizzare le prestazioni e fornire un servizio maggiormente rispettoso delle diverse culture e tradizioni. Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o care givers dell'utente diretto, particolarmente per quanto riguarda la creazione del rapporto contrattuale fra il cliente e l'Azienda fin dal momento della richiesta del servizio, spesso non proposta dal diretto interessato. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari, anche elettronici, ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi,

		anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018.
	Elementi organigramma	**Operazioni**
OPERAZIONI	**UOC Direzione Medica di Istituto - Milano**	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Direzione Medica di Istituto - Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Direzione Medica di Istituto - Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Disturbi cognitivi e Demenze Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	N.B.: sono autorizzati/incaricati del trattamento * tutti i dipendenti dell'Area Socio Sanitaria, per setting di cura, nonchè i tirocinanti/specializzandi. Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o	

	riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	interventi anche di rilievo sanitario in favore disoggetti non autosufficienti o incapaci, ivi compresi i servizi di assistenza domiciliare, accompagnamento etrasporto	nteresse pubblico rilevante
	prevenzione, diagnosi, cura e riabilitazione, ivi compresa l'assistenza degli stranieri	Consenso
	monitoraggio e sorveglianza della emergenza o riemergenza delle malattie e gestione della profilassi internazionale	nteresse pubblico rilevante
	programmazione, gestione, controllo e valutazione dell'assistenza sanitaria	nteresse pubblico rilevante
	vigilanzasulle sperimentazioni, farmacovigilanza	nteresse pubblico rilevante
	trasfusioni di sangue umano, in applicazione delle leggi, nonchè delle norme regionali vigenti in materia	nteresse pubblico rilevante
CATEGORIE E TIPOLOGIE	**Interessati**	Ospiti e utenti diversi degli Istituti geriatrici amministrati, parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute:

		attuale X pregresso X relativo a familiari dell'interessato X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando lastessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *Aziende sanitarie; *Regioni e altre P.A. di riferimento; *Aziende ospedaliere, altre strutture di ricovero e cura e assimilabili; *enti privati; *Autorità giudiziaria; *Organi ispettivi; *soggetti esterni erogatori del servizio, anche in affidamento; *tutori, curatori e amministratori disostegno; *soggetti facenti parte delle reti del FSE e della CRS, nonché degli erogatori di prestazioni per utenti cronici/fragili).Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio.In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi.E' possibile ilrecupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza -rispettoa trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale –di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative,quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative •fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	Sì
	Ultima eseguita il	-

Prossima da eseguire il	-

TRATTAMENTO	**Prestazioni di Medicina di Laboratorio**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-040331-020
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta , file system, app. gestionale, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOSD Servizi specialistici
	Autorizzati al trattamento	Tutti gli autorizzati di UOSD Servizi specialistici
	Processo	l trattamento viene posto in essere per l'effettuazione di tutte le attività correlate alla fornitura di prestazioni di medicina di laboratorio diverse su richiesta dell'interessato (anche mediante prenotazione on line. I dati vengono forniti, mediante presentazione di apposita istanza o di idonea prescrizione, dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per la gestione delle situazioni patologiche e per l'erogazione delle prestazioni agli interessati, nell'ambito delle finalità istituzionali dell'Azienda e in ottemperanza alla normativa regionale in materia. I dati etnici o relativi a particolari convinzioni religiose, filosofiche o di altro genere vengono trattati al fine di personalizzare le prestazioni e fornire un servizio maggiormente rispettoso delle diverse culture e tradizioni. Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o care givers dell'utente diretto, particolarmente per quanto riguarda la creazione del rapporto contrattuale fra il cliente e l'Azienda fin dal momento della richiesta del servizio, spesso non proposta dal diretto interessato. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOSD Servizi specialistici	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta,

	registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1.prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo2.trattare i dati secondo le modalità in uso in Azienda3.effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4.trattare i dati in modo lecito e secondo correttezza 5.attenersi alle istruzioni impartite 6.applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7.prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8.astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9.informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati10.garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza11.eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario:controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro;restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato;conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate;non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento;laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro;qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili;custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali.In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario:utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, edimpostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password);custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione;modificare la password fornita al primo accesso, e poi ogni 3 mesi;adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate;mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi;non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.),conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego daparte di soggetti non autorizzati;curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute;non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta;evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a InternetNON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similariNON utilizzare Google Drive o similariNON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari)Al proposito, si evidenzia che il Personale appartenente all'Aziendadovrà sempre: 5i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato,e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative;ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti;iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale.iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	interventidi prevenzione, diagnosi e di / Consenso

	rilievo sanitario	
CATEGORIE E TIPOLOGIE	**Interessati**	utenti interni ed esterni
	Categorie dati personali	Dati personali in sensolato, tra cui dati idonei a rivelare: -Origine razziale ed etnica X-Convinzioni religiose Xfilosofiche Xdi altro genere X-Stato di salute: attuale Xpregresso X relativo a familiari dell'interessato X
	Tipologie dati personali	Dati personali in sensolato, tra cui dati idonei a rivelare: -Origine razziale ed etnica X-Convinzioni religiose Xfilosofiche Xdi altro genere X-Stato di salute: attuale Xpregresso X relativo a familiari dell'interessato X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali, nonché ad eventuali terzi gestori di banche dati assimilabili per ambiti di categoria e finalità, in particolare al fine di instaurare sinergie in ambito socio-sanitario-assistenziale. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio.In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi.E' possibile ilrecupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in sensolato, tra cui dati idonei a rivelare: -Origine razziale ed etnica X-Convinzioni religiose Xfilosofiche Xdi altro genere X-Stato di salute: attuale Xpregresso X relativo a familiari dell'interessato X	I dati raccolti vengonoconservati nei termini previstidalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza -rispettoa trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale –di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative,quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative •fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo

		dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Prestazioni legate a servizi riabilitativi dell'età evolutiva**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-045145-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	Carta, gestionale, file system -con ausilio di strumenti elettronici -senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Direzione Medica di Istituto - Abbiategrasso
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Direzione Medica di Istituto - Abbiategrasso
	Processo	Il trattamento viene posto in essere allo scopo di fornire interventi di logopedia (per disturbi specifici del linguaggio e dell'apprendimento), di psicomotricità (per i disturbi relazionali e comportamentali e per deficit cognitivi), di riabilitazione neuro-visiva e di riabilitazione neuromotoria, interventi di psicoterapia per l'età evolutiva con possibilità di colloqui con i genitori. I dati vengono forniti, mediante presentazione di apposita istanza o di idonea prescrizione, dai soggetti che esercitano nei confronti dell'interessato la patria potestà, o rivestono la qualifica di tutori o da terzi (pediatra di riferimento, medico di base, medico delle UONPIA o dei servizi territoriali, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sensibili relativi allo stato di salute vengono trattati per la gestione delle situazioni patologiche e per l'erogazione delle prestazioni socio-sanitarie agli interessati, nell'ambito delle finalità istituzionali dell'Azienda e in ottemperanza alla normativa regionale in materia. I dati e le operazioni correlate ad eventuali attività di ricerca, specificati nei singoli progetti, qualora non sia possibile l'utilizzo di dati anonimi, sono trattati comunque in modo da non poter identificare gli interessati, a meno che l'abbinamento di tali dati identificativi al materiale di ricerca non sia temporaneo e essenziale per il risultato della ricerca, e motivato per iscritto nel progetto di ricerca. 23Al fine di instaurare e gestire le procedure connesse alle prestazioni erogate, in molti casi è necessario ed indispensabile anche il trattamento di dati dei familiari o caregivers dell'utente diretto. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.

	Elementi organigramma	Operazioni
OPERAZIONI	UOC Direzione Medica di Istituto - Abbiategrasso	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		N.B.: sono autorizzati/incaricati del trattamento * tutti i dipendenti del servizio di riabilitazione dell'età evolutiva Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1.prendere visione dei documenti aziendali di gestione della privacy SI-MOPe Registro delle Attività di Trattamento vigenti nel tempo2.trattare i dati secondo le modalità in uso in Azienda3.effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4.trattare i dati in modo lecito e secondo correttezza 5.attenersi alle istruzioni impartite 6.applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7.prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8.astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9.informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati10.garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza11.eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate;non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili;custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali.In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password);custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate;mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.),conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego daparte di soggetti non autorizzati;curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a InternetNON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari)Al proposito, si evidenzia che il Personale appartenente all'Aziendadovrà sempre: 5i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI		Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	Base giuridica
FINALITÀ, E BASI GIURIDICHE	Erogazione degli interventi riabilitativi	Interesse pubblico rilevante
	Instaurazione, gestione, pianificazione e controllo dei rapporti con laRegione Lombardia, le Aziende Sanitarie Locali e le Aziende Ospedaliere, nonché con altri soggetti accreditati o convenzionati del Servizio Sanitario Nazionale e Regionale	obblighi di legge cui è soggetto il titolare del trattamento
	Attività amministrative correlate a quelle di prevenzione,diagnosi, cura e riabilitazione dei soggetti assistiti dal SSN	obblighi di legge cui è soggetto il titolare del trattamento
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Soggetti minori affetti da disturbi del comportamento e dello spettro autistico; parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, l'attività riabilitativa ambulatoriale viene organizzata in modo tale da mantenere forme di collaborazione strutturata con Unità Neuropsichiatriche Infantili di Base, i servizi scolastici, i servizi sociali, i servizi sanitari (neuropsichiatria infantile ospedaliera, pediatri di base, altri specialisti) e le altre figure professionali dell'ambito pediatrico, per comunicazioni relative a relazioni cliniche diagnostiche, valutazioni, diagnosi funzionali, piani riabilitativi, esiti di gruppi operativi). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	

TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza -rispettoa trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale –di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative,quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative •fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente
IMPATTO	**Necessita valutazione impatto**	Sì
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Protocollo informatico, gestione dei flussi documentali, albo online**	
RISCHIO INIZIALE	**Medio (2)**	🟡
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-041646-017
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	gestionale, carta, con ausilio di strumenti elettronici senza ausilio di strumenti elettronici
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Ogni ora
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione Generale/Responsabile del Protocollo
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione Generale/Responsabile del Protocollo
	Processo	Il trattamento si svolge secondo le indicazioni di cui ai manuali di protocollo e di gestione documentale adottati in Azienda, e ai sensi delle previsioni normative in materia vigenti per la P.A.. Per quanto riguarda l'Albo on line, le procedure interne non prevedono la pubblicazione integrale o in forma estensiva di documenti e/o provvedimenti aziendali che riportino dati personali (anche di carattere particolare) non ostensibili ai sensi delle normative vigenti.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	Direzione Generale/Responsabile del Protocollo	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al	

	termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica** Dare adempimento alle disposizioni legislative in materia di protocollazione, pubblicità e gestione della documentazione per la Pubblica Amministrazione. / Compiti di interesse pubblico o connessi all'esercizio di pubblici poteri da parte dell'Azienda. Consenso
CATEGORIE E TIPOLOGIE	**Interessati**: Soggetti che si interfacciano/corrispondono con l'Azienda; soggetti che intrattengono rapporti con l'Azienda. **Categorie dati personali**: Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X **Tipologie dati personali**: Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X **Categorie di destinatari**: Strutture interne destinatarie dei documenti protocollati e dei flussi documentali. Soggetti che accedono all'Albo online. E' consentita la comunicazione dei dati ad altri soggetti

		pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali, nonché ad eventuali terzi gestori di banche dati assimilabili per ambiti di categoria e finalità, in particolare al fine di instaurare sinergie in ambito socio-sanitarioassistenziale anche con realtà afferenti al terzo settore o con qualifica di ONLUS. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Opinioni politiche X - Adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale X - Stato di salute: attuale X pregresso X relativo a familiari dell'interessato X - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Recupero crediti**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-040741-022
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	file system, carta, gestionale, con e senza ausilio di strumenti elettronici
	Numerosità degli interessati	Centinaia
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOS Avvocatura
	Autorizzati al trattamento	Tutti gli autorizzati di UOS Avvocatura
	Processo	I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia e presso eventuali altre strutture aziendali interessate, e secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOS Avvocatura	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di	

	trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione — obblighi di legge cui è soggetto il titolare del trattamento
	attività di recupero delle posizioni debitorie nei confronti dell'Azienda — legittimo interesse prevalente del titolare o di terzi cui i dati vengano comunicati
CATEGORIE E TIPOLOGIE	**Interessati** — Utenti, familiari, obbligati per legge; inquilini e affittuari stabili civili e fondi rustici; dipendenti, collaboratori a qualsiasi titolo, amministratori., Creditori diversi
	Categorie dati personali — Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X
	Tipologie dati personali — Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X

CONSERVAZIONE	**Categorie di destinatari**	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte; *Studi legali; *Cancellerie uffici giudiziari; *Agenzia delle Entrate e del Territorio). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale. Per le operazioni gestite dalla UOS Avvocatura e Gestione Legale si applicano le disposizioni di cui all'art. 4 dell'All. 1 della Delibera del Garante della Privacy n. 512 del 19.12.2018
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Registrazione riunioni e sedute del Consiglio (in presenza/da remoto/miste)**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2023-Azi-070537-032
	Date	Creato il 09/03/2023, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta gestionale con ausilio di strumenti elettronici senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Mensilmente
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione generale
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione generale
	Processo	La videoconferenza può essere oggetto di registrazione al solo fine di consentire una corretta verbalizzazione della riunione. La registrazione ha mero valore di ausilio per il verbalizzante. Il collegamento da remoto da parte del partecipante vale quale consenso espresso al conferimento ed al trattamento dei dati personali connessi. Ai fini della registrazione audio-video il consenso viene espresso esplicitamente in avvio di seduta, e viene riportato a verbale. Il rifiuto a prestare il consenso alla registrazione da parte di un soggetto legittimato a partecipare alla riunione non potrà essere causa di esclusione dalla stessa, ma produrrà il solo effetto che la riunione non potrà essere registrata
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	Direzione generale	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI		Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle

	sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	Partecipazione a incontri, riunioni, sedute del Consiglio in videoconferenza e da remoto — consenso esecuzione di compito di interesse pubblico o connesso all'esercizio di pubblici poteri da parte dell'Azienda
	Registrazione audio-video di incontri, riunioni, sedute del Consiglio — consenso esecuzione di compito di interesse pubblico o connesso all'esercizio di pubblici poteri da parte dell'Azienda
CATEGORIE E TIPOLOGIE	**Interessati** — Partecipanti da remoto a incontri, riunioni, sedute del Consiglio – registrazioni audio/video
	Categorie dati personali — Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X
	Tipologie dati personali — Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X
	Categorie di destinatari — Non sono consentite la comunicazione e diffusione dei dati ad altri soggetti pubblici o privati. Gli stessi vengono utilizzati esclusivamente per lo svolgimento delle finalità di riferimento da parte dei soli soggetti aziendali autorizzati al trattamento. ferma restando la facoltà dei partecipanti di accedere alle registrazioni stesse per verificare la coerenza dei propri interventi rispetto a quanto riportato nel verbale stesso.
CONSERVAZIONE	**In caso di crash, dati disponibili entro** — L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul

		Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X	I dati audio-video correlati alla mera partecipazione da remoto non sono conservati. I supporti di registrazione cessano di essere conservati una volta approvato e sottoscritto il relativo verbale. Qualora il Consiglio opti per la conservazione della registrazione delle sedute oltre il periodo sopra indicato, i dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Rilascio di autorizzazioni per l'utilizzo di spazi aziendali**	
RISCHIO INIZIALE	**Medio (2)**	🟡
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-043239-029
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system, gestionale con ausilio di strumenti elettronici senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Milano, UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Milano, Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	Il trattamento dei dati è finalizzato a instaurare il rapporto, sino alla conclusione dello stesso e all'espletamento degli incombenti connessi. I dati sono oggetto di trattamento presso le strutture organizzative rispettivamente competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. Vengono gestite interconnessioni interne alla struttura e – se previste – con altri Enti pubblici. La raccolta dei dati avviene principalmente presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Operativa Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o

		qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - con altri trattamenti o archivi dello stesso titolare X interconnessione, raffronti di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: □ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; □ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; □ conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; □ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; □ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; □ qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; □ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; □ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; □ richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: □ utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); □ custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; □ modificare la password fornita al primo accesso, e poi ogni 3 mesi; □ adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; □ mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; □ non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), □ conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; □ curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; □ non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; □ evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet □ NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari □ NON utilizzare Google Drive o similari □ NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
RESPONSABILI	**Ragione sociale**	**Attività**
	UOC Affari Generali Dirigente	attività della UOC Affari Generali e Trasparenza

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	Instaurazione di rapporti con soggetti terzi per l'utilizzo a titolo gratuito o oneroso di spazi aziendali (sale, uffici, spazi esterni)	adempimento di obblighi precontrattuali e contrattuali -
	adempiere alle disposizioni in materia di trasparenza e prevenzione della corruzione	obblighi di legge cui è soggetto il titolare del trattamento -
CATEGORIE E TIPOLOGIE	**Interessati**	Soggetti pubblici/privati e del Terzo Settore interessati all'utilizzo di spazi aziendali.
	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Dati giudiziari X
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Dati giudiziari X
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare,*Autorità Giudiziaria; *consulenti tecnici incaricati dall'Autorità Giudiziaria; *Autorità di vigilanza sui contratti; *Forze di Polizia; *Società assicuratrici; *incaricati di indagini difensive proprie e altrui, società di recupero crediti; *consulenti della controparte; *eventuali Amministrazioni coinvolte *Agenzia delle entrate; *tutori, curatori e amministratori di sostegno). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche X di altro genere X - Dati giudiziari X	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne;

		assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Sito web e social media aziendali**	
RISCHIO INIZIALE	**Basso (1)**	●
RISCHIO RIDOTTO	**Basso (1)**	●
RISCHIO	**Basso**	● Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-045038-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	file system, carta, app. gestionale, cloud Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	L'invio di messaggi agli indirizzi di contatto indicati sul sito e di messaggi privati indirizzati ai profili istituzionali dell'Azienda sui social media comporta l'acquisizione di tutti i dati personali inclusi volontariamente dal mittente nel testo della propria comunicazione. I dati inseriti sono trasmessi ai Responsabili del trattamento competenti per materia.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: □ controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; □ restituire gli atti ed i documenti al	

	termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli
FINALITÀ, E BASI GIURIDICHE	**Finalità** / **Base giuridica**
	ricevere e dar riscontro a richiesta di contatto - corretto funzionamento del sito internet / Consenso
	funzionamento dei social media / Consenso
CATEGORIE E TIPOLOGIE	**Interessati** / Soggetti che consultano il sito istituzionale e che usufruiscono dei servizi proposti
	Categorie dati personali / Tutti i dati personali inclusi volontariamente dal mittente nel testo della propria comunicazione. Dati anagrafici di tipo comune (nome, cognome, data di nascita, codice fiscale, contatto telefonico e indirizzo e-mail) comunicati attraverso la compilazione dei form disponibili nelle sezioni del sito, dati sensibili e giudiziari inclusi nelle comunicazioni volontarie, o dati rilevabili in conseguenza dell'utilizzo dei social media aziendali, nonché eventuali ulteriori dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet.
	Tipologie dati personali / Tutti i dati personali inclusi volontariamente dal mittente nel testo della propria comunicazione. Dati anagrafici di tipo comune (nome, cognome, data di nascita, codice fiscale, contatto telefonico e indirizzo e-mail) comunicati attraverso la compilazione dei form disponibili nelle sezioni del sito, dati sensibili e giudiziari inclusi nelle comunicazioni volontarie, o dati rilevabili in conseguenza dell'utilizzo dei social media aziendali, nonché eventuali ulteriori dati personali la cui trasmissione è implicita nell'uso

		dei protocolli di comunicazione di internet.
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali, nonché ad eventuali terzi gestori di banche dati assimilabili per ambiti di categoria e finalità, in particolare al fine di instaurare sinergie in ambito socio-sanitario-assistenziale anche con realtà afferenti al terzo settore o con qualifica di ONLUS. Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
	In caso di crash, dati disponibili entro	In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
CONSERVAZIONE	**Tutti i dati personali inclusi volontariamente dal mittente nel testo della propria comunicazione. Dati anagrafici di tipo comune (nome, cognome, data di nascita, codice fiscale, contatto telefonico e indirizzo e-mail) comunicati attraverso la compilazione dei form disponibili nelle sezioni del sito, dati sensibili e giudiziari inclusi nelle comunicazioni volontarie, o dati rilevabili in conseguenza dell'utilizzo dei social media aziendali, nonché eventuali ulteriori dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet.**	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente

IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**URP e gestione dei reclami**	
RISCHIO INIZIALE	**Basso (1)**	
RISCHIO	**Basso**	Il valore di rischio è stato calcolato tramite **Pre valutazione del trattamento**
GENERALI	**Identificativo**	2022-Azi-043531-031
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	Carta, app. gestionale, file system, Con ausilio di strumenti elettronici Senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Ogni giorno
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	Il trattamento viene posto in essere per l'effettuazione di tutte le attività di competenza degli uffici di relazione con il pubblico (gestione di osservazioni, richieste di chiarimenti, opposizioni, denunce o reclami inerenti all'attività e alle prestazioni aziendali; fornire agli utenti ed alle persone interessate informazioni inerenti l'attività istituzionale, il funzionamento dell'Azienda e le prestazioni erogate). I I dati vengono forniti dall'interessato o da terzi (familiari o persone di riferimento, tutori, curatori, amministratori di sostegno, medico di base, ASL, Comune, Autorità diverse, etc.) e possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente. I dati sono oggetto di trattamento presso le strutture organizzative competenti per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Le informazioni relative alle prestazioni erogate sono strutturate in cartelle cliniche e/o fascicoli sociosanitari ai sensi delle vigenti disposizioni regionali in materia. Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. I dati possono pervenire all'Azienda anche su comunicazione di soggetti terzi, anche con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi ai sensi del DPR 445/2000. Per i dati relativi alle persone decedute si rimanda alle corrispondenti previsioni di cui al D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	N.B.: sono autorizzati/incaricati del trattamento tutti i dipendenti assegnati all'Ufficio Relazioni con il Pubblico e agli sportelli Relazioni con il Pubblico presenti nelle diverse sedi di lavoro. Ciascun dipendente formalmente assegnato alla struttura organizzativa o preposto	

	allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli

	Finalità	**Base giuridica**
FINALITÀ, E BASI GIURIDICHE	attività svolte dagli Uffici Relazioni con il Pubblico	obblighi di legge cui è soggetto il titolare del trattamento
	gestione delle istanze, reclami, suggerimenti ed elogi	adempimento di obblighi precontrattuali e contrattuali
CATEGORIE E TIPOLOGIE	**Interessati**	Ospiti e utenti diversi degli Istituti geriatrici amministrati, parenti, familiari, care givers, amministratori di sostegno, curatori, tutori.

	Categorie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose filosofiche di altro genere - Stato di salute: attuale pregresso relativo a familiari dell'interessato
	Tipologie dati personali	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica - Convinzioni religiose filosofiche di altro genere - Stato di salute: attuale pregresso relativo a familiari dell'interessato
	Categorie di destinatari	E' consentita la comunicazione dei dati ad altri soggetti pubblici e privati in esecuzione di previsioni normative o quando la stessa è comunque necessaria per lo svolgimento di funzioni istituzionali (in particolare, *Aziende sanitarie; *Regioni e altre P.A. di riferimento; *Aziende ospedaliere, altre strutture di ricovero e cura e assimilabili; *enti privati; *Autorità giudiziaria; *Organi ispettivi; *soggetti esterni erogatori del servizio, anche in affidamento; *tutori, curatori e amministratori di sostegno; *soggetti facenti parte delle reti del FSE e della CRS, nonché degli erogatori di prestazioni per utenti cronici/fragili). Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica anche a terzi unicamente i dati necessari per l'instaurazione e la completa gestione dei rapporti in essere, nonché per l'esercizio del diritto di difesa in giudizio.
CONSERVAZIONE	**In caso di crash, dati disponibili entro**	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati personali in senso lato, tra cui dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose filosofiche di altro genere - Stato di salute: attuale pregresso relativo a familiari dell'interessato	I dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale.
ASSET	**Del titolare**	[Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.

IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Videosorveglianza**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-025631-011
	Date	Creato il 26/10/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	su supporto video
	Numerosità degli interessati	Migliaia
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale
	Elementi organigramma	UOC Gestione Operativa Milano, UOC Gestione Operativa Abbiategrasso-Vimodrone
	Autorizzati al trattamento	Tutti gli autorizzati di UOC Gestione Operativa Milano, Tutti gli autorizzati di UOC Gestione Operativa Abbiategrasso-Vimodrone
	Processo	Il servizio di videosorveglianza degli accessi e di altre zone nevralgiche delle strutture aziendali è effettuato al fine di monitorare eventuali situazioni a rischio per la sicurezza di utenti, visitatori e dipendenti, e a salvaguardia del patrimonio aziendale. I dati idonei a rilevare lo stato di salute, l'appartenenza etnica o razziale e le convinzioni religiose sono rilevati soltanto incidentalmente attraverso la ripresa dei tratti somatici, dell'abbigliamento degli interessati o del contesto in cui viene effettuata la ripresa. I dati eventualmente registrati possono essere trasmessi esclusivamente all'Autorità giudiziaria o di Pubblica Sicurezza dietro espressa richiesta. I dati sono oggetto di trattamento presso la struttura organizzativa competente per materia, secondo le disposizioni interne vigenti nel tempo, cui si fa espresso rimando. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. La raccolta dei dati avviene presso i diretti interessati; l'informativa agli stessi, e l'acquisizione del consenso nei casi prescritti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia.
OPERAZIONI	**Elementi organigramma**	**Operazioni**
	UOC Gestione Operativa Milano	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	UOC Gestione Operativa Abbiategrasso-Vimodrone	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o

		qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	Sono autorizzati/incaricati del trattamento tutti i dipendenti addetti ai servizi generali e alle portinerie/reception degli istituti. Ciascun dipendente formalmente ivi assegnato riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, per la sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite: 1. prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. 4 In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: 5 i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**
	sicurezza e protezione di persone e beni	obblighi di legge cui è soggetto il titolare del trattamento
CATEGORIE E TIPOLOGIE	**Interessati**	Tutti coloro che transitano in prossimità degli accessi alla struttura e/o che entrano negli

CONSERVAZIONE		Istituti
	Categorie dati personali	Dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche di altro genere - Stato di salute: attuale X
	Tipologie dati personali	Dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche di altro genere - Stato di salute: attuale X
	Categorie di destinatari	Nello svolgimento delle proprie funzioni istituzionali l'Azienda comunica ad altri soggetti pubblici (in particolare, * Autorità giudiziaria e di P.S. dietro specifica richiesta) e anche a terzi unicamente i dati necessari in esecuzione di previsioni normative e per l'attuazione delle finalità di sorveglianza e tutela, nonché per l'esercizio del diritto di difesa in giudizio
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
	Dati idonei a rivelare: - Origine razziale ed etnica X - Convinzioni religiose X filosofiche di altro genere - Stato di salute: attuale X	2 giorni
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Server] Server (SRV-0001), [Software] Software (SFT-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	No
	Ultima eseguita il	-
	Prossima da eseguire il	-

TRATTAMENTO	**Whistleblowing**	
RISCHIO INIZIALE	**Alto (3)**	🔴
RISCHIO RIDOTTO	**Basso (1)**	🟢
RISCHIO	**Basso**	🟢 Il valore di rischio è stato calcolato tramite **Applicazione delle misure tecniche ed organizzative**
GENERALI	**Identificativo**	2022-Azi-044537-033
	Date	Creato il 10/12/2022, modificato il 28/10/2026
	Stato	attivo
	Modalità di gestione	carta, file system con ausilio di strumenti elettronici senza ausilio di strumenti elettronici
	Numerosità degli interessati	Decine
	Frequenza del trattamento	Non periodico
	Forma del dato	Digitale e cartacea
	Elementi organigramma	UOC Affari Generali, Responsabile della Prevenzione della Corruzione e per la Trasparenza
	Autorizzati al trattamento	Tutti gli autorizzati con mansione di Dirigente UOC, Tutti gli autorizzati con mansione di Responsabile di Responsabile della Prevenzione della Corruzione e per la Trasparenza
	Processo	I dati personali relativi alle segnalazioni di violazioni del Piano anticorruzione sono trattati dal Responsabile della prevenzione della corruzione e della trasparenza nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse dell'integrità dell'Azienda. Per le modalità di segnalazione, e le relative procedure, si rimanda al MOGC vigente nel tempo e disponibile sul sito aziendale. A tutela del whistleblower restano ferme le misure generali di cui alle lettere A e B del punto 7 del vigente MOP, e inoltre: - occorre rispettare i principi di liceità, correttezza, trasparenza e minimizzazione dei dati - i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Sussiste, in ogni caso, il divieto di rilevare l'identità del segnalante con riferimento non solo al nominativo del medesimo ma anche a tutti gli elementi della segnalazione, inclusa la documentazione ad essa allegata, nella misura in cui il loro disvelamento, anche indirettamente, possa consentire l'identificazione del segnalante., Qualora, per ragioni istruttorie, altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata, il trattamento dei dati va improntato alla massima cautela, a cominciare dall'oscuramento dei dati medesimi, specie quelli relativi al segnalante. Vanno, in ogni caso, adottate cautele particolari al fine di evitare la indebita circolazione di informazioni personali anche all'interno degli uffici dell'amministrazione in capo a soggetti non autorizzati al trattamento dei dati. Le segnalazioni sono oggetto di protocollazione in registro riservato. Il trattamento viene effettuato mediante operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione e distruzione di dati, anche se non registrati in una banca dati, con o senza l'ausilio di strumenti elettronici. La raccolta dei dati avviene presso i diretti interessati. L'informativa specifica agli interessati e l'eventuale acquisizione del consenso sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia. Il trattamento di dati personali viene effettuato anche per i dati connessi alle segnalazioni di infrazione del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01, ricadenti sotto la responsabilità e le competenze dell'Organismo di Vigilanza sul medesimo. Per le modalità di segnalazione, e le relative

		procedure, si rimanda al MOGC vigente nel tempo e disponibile sul sito aziendale
	Elementi organigramma	**Operazioni**
OPERAZIONI	**UOC Affari Generali**	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
	Responsabile della Prevenzione della Corruzione e per la Trasparenza	- raccolta diretta presso l'interessato X - acquisizione da altri soggetti esterni X - raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione X Operazioni particolari - interconnessione, raffronti con altri trattamenti o archivi dello stesso titolare X di altri titolari X - comunicazione X
ISTRUZIONI	1.prendere visione dei documenti aziendali di gestione della privacy SI-MOP e Registro delle Attività di Trattamento vigenti nel tempo 2. trattare i dati secondo le modalità in uso in Azienda 3. effettuare le sole attività di trattamento necessarie allo svolgimento della propria mansione 4. trattare i dati in modo lecito e secondo correttezza 5. attenersi alle istruzioni impartite 6. applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali 7. prevenire e/o evitare la comunicazione o diffusione illecita dei dati 8. astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati 9. informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati 10. garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche dopo la cessazione dell'incarico, alcuna delle informazioni di cui si è venuti a conoscenza 11. eseguire ogni altra istruzione che sia eventualmente impartita dal Responsabile del Trattamento in occasioni specifiche. In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario: controllare e custodire gli atti ed i documenti contenenti dati personali durante la sessione di lavoro; restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato; conservare gli atti ed i documenti contenenti dati sensibili in cassetti e/o armadi chiusi a chiave e/o in qualsiasi altro luogo ad accesso limitato alle sole persone autorizzate; non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento; laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro; qualora non occorra più conservarle, distruggere le copie cartacee in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili; custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente; prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni; richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali. In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario: utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password); custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione; modificare la password fornita al primo accesso, e poi ogni 3 mesi; adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate; mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi; non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.), conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati; curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute; non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta; evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari NON utilizzare Google Drive o similari NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, supersensibili e giudiziari) Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre: i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative; ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti; iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale. iv. utilizzare le proprie competenze tecnico-informatiche per	

	salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso. v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al vigente MOP, nell'esecuzione del lavoro.	
TITOLARI	Azienda di Servizi alla Persona Golgi-Redaelli	
FINALITÀ, E BASI GIURIDICHE	**Finalità**	**Base giuridica**
	effettuare le attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti	Interesse pubblico rilevante
CATEGORIE E TIPOLOGIE	**Interessati**	Soggetti che effettuano segnalazioni volte a denunciare comportamenti connessi a un possibile rischio corruttivo, nonché a violazioni del Modello Organizzativo aziendale ex D. Lgs. 231/2001, e loro facilitatori (dipendenti dell'ASP, lavoratori autonomi e collaboratori, liberi professionisti e consulenti, lavoratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'ASP, volontari, tirocinanti, amministratori, colleghi, parenti o affetti stabili di chi ha segnalato). Soggetti segnalati. Altri soggetti coinvolti.
	Categorie dati personali	Dati personali del segnalante, inseriti nella denuncia o nella apposita piattaforma informatica dedicata alla ricezione delle segnalazioni, nonché dati personali presenti nella segnalazione, inclusa la documentazione ad essa allegata. Nell'ambito delle segnalazioni vengono trattati dati anche relativi al soggetto segnalato o ad altri soggetti coinvolti dalla segnalazione e possono riguardare dati comuni ed anche particolari e relativi a reati ed irregolarità.
	Tipologie dati personali	Dati personali del segnalante, inseriti nella denuncia o nella apposita piattaforma informatica dedicata alla ricezione delle segnalazioni, nonché dati personali presenti nella segnalazione, inclusa la documentazione ad essa allegata. Nell'ambito delle segnalazioni vengono trattati dati anche relativi al soggetto segnalato o ad altri soggetti coinvolti dalla segnalazione e possono riguardare dati comuni ed anche particolari e relativi a reati ed irregolarità
	Categorie di destinatari	L'Azienda di Servizi alla Persona "Golgi-Redaelli", qualora ritenga la segnalazione fondata in un'ottica di prevenzione della corruzione e di rispetto delle previsioni MOGC, può disporre l'invio della segnalazione alle istituzioni competenti, quali ad esempio e tra gli altri, l'Ispettorato per la Funzione Pubblica, la Corte dei conti, l'Autorità giudiziaria, la Guardia di Finanza, l'ANAC.
	In caso di crash, dati disponibili entro	L'infrastruttura prevede le ridondanze delle componenti hardware tali da garantire in generale la continuità del servizio. In caso di crash dell'intero sistema tale da non consentire l'accesso ai dati in esso contenuti, è possibile il recupero da un NAS in tempi brevi. E' possibile il recupero delle medesime informazioni anche da spazio dedicato sul Cloud. In tal caso i tempi di recupero sono di durata media.
CONSERVAZIONE	**Dati personali del segnalante, inseriti nella denuncia o nella apposita piattaforma informatica dedicata alla ricezione delle segnalazioni, nonché dati personali presenti nella segnalazione, inclusa la documentazione ad essa allegata. Nell'ambito delle segnalazioni vengono trattati dati anche relativi al soggetto segnalato o ad altri soggetti coinvolti dalla segnalazione e possono riguardare dati comuni ed anche particolari e relativi a reati ed irregolarità.**	dati raccolti vengono conservati nei termini previsti dalle normative vigenti in materia di Aziende di Servizi alla Persona, di Pubblica Amministrazione e, in ogni caso, per necessità di carattere storico-archivistico e documentale. In particolare, le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione, e comunque non oltre i 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.
ASSET	**Del titolare**	[Apparati di rete] apparati di rete (PPR-0001), [Archivio] archivi informatici e cartacei (RCH-0001), [Armadio con serratura] armadio con serratura (RMD-0001), [Database] database (DTB-0001), [Dispositivi di backup] Dispositivi di backup (DSP-0001), [Scanner multifunzione] Scanner multifunzione (SCN-0001), [Schedario] Schedario (SCH-0001),

		[Server] Server (SRV-0001), [Software] Software (SFT-0001), [Stampanti] Stampanti (STM-0001), [Desktop] Desktop (DSK-0001)
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
MISURE TECNICHE E ORGANIZZATIVE	**Trattamento**	Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante misure tecniche, organizzative e di sicurezza - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati. In particolare, vengono adottate tra le altre le seguenti principali misure: • organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative • fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti • logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione. Per il dettaglio delle misure relative a diversi trattamenti si rimanda al SI-MOP aziendale vigente.
IMPATTO	**Necessita valutazione impatto**	Sì
	Ultima eseguita il	08/06/2023
	Prossima da eseguire il	07/06/2024

Azienda di Servizi alla Persona Golgi-Redaelli IT04737420150
Via Bartolomeo d'Alviano, n.78 - 20146, Milano (MI) - Italia
+39 02 7251 81 direzionegenerale@golgiredaelli.it