Istituto Romano di San Michele
Azienda Pubblica di Servizi alla Persona
00147 – Piazzale Antonio Tosti n.4

ASP - Istituto Romano di San Michele

Privacy Policy

Versione n. 1.0 del 24/08/2023

INDICE

PREMESSA

La presente policy si pone l'obiettivo di descrivere sommariamente i trattamenti e le operazioni che il personale dell'ASP Istituto Romano di San Michele (di seguito, anche «*l'Istituto*», *"Azienda"*) deve svolgere in merito alle varie categorie di dati trattati, nonché le modalità di svolgimento da utilizzare affinché i trattamenti siano conformi a quanto previsto dal Regolamento UE 679/2016 (di seguito, «*il Regolamento*»).

La policy è rivolta a tutti i **dipendenti** e i **soggetti che comunque collaborano stabilmente o svolgono trattamenti per conto dell'Azienda** (di seguito cumulativamente, «*Incaricati*»), i quali pertanto sono obbligati a rispettarne le prescrizioni, i primi interamente, i secondi per la parte rilevante o a loro relativa, determinata in base al ruolo rivestito.

La policy è soggetta ad aggiornamento periodico nelle forme e nei tempi in essa indicati.

1. DEFINIZIONI

Ai fini della presente policy i termini di seguito specificati hanno il significato riportato nel presente paragrafo:

- **Regolamento** o **GDPR** è il Regolamento UE 679/2016;
- **Trattamento** è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Dato personale** è qualsiasi informazione riguardante una persona fisica identificata o identificabile («*interessato*»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Responsabile Generale del trattamento** o **Responsabile Generale**, è il soggetto incaricato a sovraintendere a tutte le operazioni di trattamento per contro del Titolare, nominato ai sensi dell'art. 28 del Regolamento;
- **Responsabile esterno** è il soggetto terzo nominato *ex* art. 28 del Regolamento che svolge uno o più trattamenti per conto del Titolare, in un ambito specifico;
- **Soggetti autorizzati al trattamento** sono i dipendenti dell'Azienda che svolgono trattamenti per conto della stessa in virtù delle loro funzioni e di specifica nomina;
- ***Data breach*** o **violazione dei dati** è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **Interessati** o **soggetti interessati** sono i soggetti i cui dati personali sono sottoposti a trattamento.

2. RUOLI E FUNZIONI IN MATERIA DI PRIVACY

Alla data di pubblicazione del presente documento sono stati assegnati, internamente all'organizzazione aziendale, i seguenti ruoli e funzioni:

- Responsabile Generale del trattamento è il Direttore – Dott. Fabio Liberati (Deliberazione del CDA n. 78 del 22 dicembre 2021);
- Responsabile della protezione dei dati personali è il DPO – Dott.ssa Serena Desidera (Decreto Commissario Straordinario n. 42 del 2 dicembre 2019);
- i ruoli di soggetti autorizzati al trattamento di:

- curricula, dati anagrafici, reddituali, contabili/fiscali, dati giudiziari, identificativi e di contatto, disciplinari, relativi a ferie, malattie, congedi, permessi, infortuni, stato di salute del personale e dei relativi familiari a seconda del tipo di permesso;
- curricula, dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, dei tirocinanti/stagisti nonché dei collaboratori e consulenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di servizi e/o forniture;
- curricula, dati anagrafici, reddituali, contabili/fiscali, identificativi e di contatto, dei componenti dei vertici politici e amministrativi;

sono assegnati ai dipendenti del Servizio Risorse Umane;

- i ruoli di soggetti autorizzati al trattamento di:

- dati anagrafici, curricula, dati contabili/fiscali del personale dipendente, dei tirocinanti/stagisti, dei collaboratori/consulenti, dei componenti dei vertici politici e amministrativi, fornitori/partner, ospiti della Casa di Riposo e della RSA e loro familiari/referenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti agli affittuari e ai rappresentanti delle società affidatarie di appalti di servizi e/o forniture;

sono assegnati ai dipendenti del Servizio Bilancio e Rendicontazione;

- i ruoli di soggetti autorizzati al trattamento di:

- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di lavori, servizi e/o forniture;
- dati anagrafici, contabili/fiscali, giudiziari, identificativi e di contatto, relativi ai conduttori degli immobili locati dall'Azienda;
- curricula, dati anagrafici, identificativi e di contatto, relativi al rapporto con l'Istituto, dei collaboratori e consulenti;
- dati anagrafici, identificativi e di contatto, afferenti allo stato di salute dei dipendenti del Servizio Patrimonio e Beni Storico Artistici;
- curricula, dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto dei collaboratori e consulenti;

sono assegnati ai dipendenti del Servizio Patrimonio e Beni Storico Artistici;

- i ruoli di soggetti autorizzati al trattamento di:

- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di lavori, servizi e/o forniture;
- dati anagrafici, identificativi e di contatto, afferenti allo stato di salute dei dipendenti del Servizio Tecnico Manutentivo, Progettazione;
- curricula, dati anagrafici, identificativi e di contatto, relativi al rapporto con l'Istituto, dei collaboratori e consulenti;

sono assegnati ai dipendenti del Servizio Tecnico Manutentivo, Progettazione;

- i ruoli di soggetti autorizzati al trattamento di:

- dati anagrafici, identificativi e di contatto, afferenti allo stato di salute dei dipendenti dell'Azienda;
- curricula, dati anagrafici, identificativi e di contatto, relativi al rapporto con l'Istituto, dei collaboratori e consulenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di servizi e/o forniture;

sono assegnati al Responsabile del Servizio Salute e Sicurezza;

- i ruoli di soggetti autorizzati al trattamento di:

- curricula, dati anagrafici, identificativi e di contatto, relativi al rapporto con l'Istituto, dei collaboratori e consulenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di servizi e/o forniture;
- dati identificativi e di navigazione internet del sito web istituzionale;
- dati identificativi e log dei sistemi informatici aziendali;

sono assegnati al dipendente dell'Ufficio ICT in Staff alla Direzione;

- i ruoli di soggetti autorizzati al trattamento di:

- curricula, dati anagrafici, identificativi e di contatto, relativi al rapporto con l'Istituto, dei collaboratori e consulenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di lavori, servizi e/o forniture;
- dati identificativi, di contatto utenti del sito web istituzionale;

sono assegnati ai dipendenti dell'Ufficio Comunicazione / URP / Internal Audit e Controllo di Gestione in Staff alla Direzione;

- i ruoli di soggetti autorizzati al trattamento di:

- curricula, dati anagrafici, identificativi e di contatto, relativi al rapporto con l'Istituto, dei collaboratori e consulenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di lavori, servizi e/o forniture;
- curricula, dati anagrafici, reddituali, contabili/fiscali, dati giudiziari, identificativi e di contatto, disciplinari, relativi a ferie, malattie, congedi, permessi, infortuni, stato di salute del personale e dei relativi familiari a seconda del tipo di permesso;
- curricula, dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, dei tirocinanti/stagisti nonché dei collaboratori e consulenti;

- curricula, dati anagrafici, reddituali, contabili/fiscali, identificativi e di contatto, dei componenti dei vertici politici e amministrativi;
- dati anagrafici, identificativi e di contatto, reddituali, contabili/fiscali, afferenti allo stato di salute, dati giudiziari, relativi agli ospiti della Casa di Riposo e della RSA e ai loro parenti;

sono assegnati ai dipendenti dell'Ufficio Affari Generali e Compliance in Staff alla Direzione;

- i ruoli di soggetti autorizzati al trattamento di:
- dati anagrafici, identificativi e di contatto, reddituali, contabili/fiscali, afferenti allo stato di salute, dati giudiziari, relativi agli ospiti della Casa di Riposo e della RSA e ai loro parenti;
- dati anagrafici, identificativi e di contatto, afferenti allo stato di salute dei dipendenti dell'Area Servizi alla Persona;
- curricula, dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, dei tirocinanti/stagisti nonché dei collaboratori e consulenti;
- dati anagrafici, contabili/fiscali, identificativi e di contatto, relativi al rapporto con l'Istituto, afferenti ai rappresentanti delle società affidatarie di appalti di servizi e/o forniture;

sono assegnati ai dipendenti dell'Area Servizi alla Persona e Ufficio Ammissioni.

Sono stati altresì nominati, con espressa nomina, Responsabili esterni del trattamento i fornitori dell'Istituto che trattano dati personali per conto dell'Istituto stesso.

3. PRINCIPI IN MATERIA DI TRATTAMENTO

Tutti i trattamenti svolti dagli Incaricati dovranno essere improntati ai seguenti principi:

a) i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («*liceità, correttezza e trasparenza*»);
b) i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, del Regolamento considerato incompatibile con le finalità iniziali («*limitazione della finalità*»);
c) i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («*minimizzazione dei dati*»);
d) i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («*esattezza*»);
e) i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 citato, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («*limitazione della conservazione*»);
f) i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («*integrità e riservatezza*»).

Qualora una determinata operazione non sia normata dalla presente policy gli Incaricati dovranno operare secondo i principi di cui sopra e, nel caso in cui si ravvisi che una o più operazioni poste in essere dall'Istituto oppure descritte nella presente policy siano contrarie ai principi di cui sopra, l'Incaricato dovrà darne immediata comunicazione al Responsabile Generale.
Le seguenti procedure sono state identificate dall'Azienda nel rispetto dei principi di cui al presente punto e di quanto previsto dalla legislazione in materia di privacy vigente.

4. DESCRIZIONE DELL'ORGANIZZAZIONE AZIENDALE RELATIVA AL TRATTAMENTO DEI DATI: STRUTTURA FISICA E INFORMATICA

L'Istituto Romano di San Michele è la più grande Azienda Pubblica di Servizi alla Persona (ASP) di Roma, per rilevanza patrimoniale e attività di assistenza svolta. L'organizzazione aziendale prevede la possibilità di conservare e trattare i dati di tutti i soggetti interessati sia su supporto cartaceo che su supporto digitale.
L'Istituto Romano di San Michele gestisce un'eterogenea quantità di dati in svariate modalità e con l'ausilio di molteplici software facenti capo a dei server ubicati in Italia ed in Europa.
Il server principalmente utilizzato è custodito in ambiente cloud (Datacenter di Milano), questa infrastruttura è attiva dal 01 marzo 2023 (in precedenza era utilizzato un datacenter gruppo B) ed ospita al suo interno n. 2 VM (Virtual machine) che rispettivamente fungono da DC (Domani controller con active directory) e da File server con all'interno cartelle condivise utilizzate dai soli utenti autorizzati per settore/ufficio.
Quest'ultima VM ospita tipologie di dati personali e particolari, in quanto sono installati in essa programmi di gestione ed archiviazione dati (criptati) di magazzino, di presenze e di patrimonio mobiliare ed immobiliare.
La policy utilizzata per questo Virtual data center (VDC) prevede un back-up incrementale giornaliero full con retention di due settimane e grazie ad un ecosistema integrato costituito da 15 Data Center garantisce compliant ai massimi livelli (Tier 5 e 6) come indicato da AgID nelle Linee Guida per il Disaster Recovery nella Pubblica Amministrazione.
Per quanto afferisce alla gestione dei dati su supporto cartaceo ogni ufficio dell'Istituto ha un proprio archivio fisico con accesso limitato.

5. PROCEDURE RELATIVE ALLE VARIE CATEGORIE DI DATI TRATTATI: LE MODALITÀ DI TRATTAMENTO

Di seguito si espone un elenco sinteticamente descrittivo dei servizi in cloud gestiti all'Istituto con la tipologia di dati trattati:

- **Software gestione contabilità (dati personali)**

- per scelta strategico/aziendale i dati utilizzati in ambito contabile sono custoditi all'interno del database locale ubicato nell'ufficio ragioneria gestito dalla Soc.TP One S.r.l., la quale ne garantisce i corretti back-up giornalieri ed al contempo la sicurezza informatica;

- **Software gestione della fiscalità (dati personali)**

- questa branca della contabilità viene gestita in un server Cloud dalla Società Wolters Kluwer Italia S.r.l. che gestisce e conserva dati con i relativi backup;

- **Software gestione protocollo informatico (dati personali e particolari)**

- all'interno di questo importante strumento transitano e sono conservati variegati tipi di dati, la piattaforma telematica viene gestita dalla Società Dedanext S.p.A. attraverso la suite Civilia Next, la quale si appoggia su piattaforma di cloud computing Microsoft Azure, conforme alle leggi sulla privacy contenute nel modello UE;

- **Software di gestione cartella clinica informatizzata (dati personali e dati particolari)**

- dal 05 dicembre 2022 l'Istituto utilizza una piattaforma di gestione informatica delle cartelle sanitarie associate agli ospiti della Casa di Riposo e della RSA. Questa infrastruttura (denominata *THE.0*), in grado di mettere in co-operazione personale assistenziale e sanitario, viene gestita dalla Società Netpolaris S.r.l. Il software è allineato alle principali linee guida e alle normative in materia di privacy ed i sui server sono ubicati in Germanie e Finlandia;

- **Conservazione registro di protocollo e fatture (dati personali)**

- il servizio di conservazione sostitutiva delle fatture passive (art. 6 c. 7 del DPCM 3 dicembre 2013 *e s.m.i.*) ed il servizio di conservazione sostitutiva del protocollo giornaliero (ai sensi dell'art. 6 c. 7 del DPCM 3 dicembre 2013 *e s.m.i.*) è stato affidato alla società Enerj s.r.l. grazie all'interoperabilità con la suite messa a disposizione dalla Soc. Dedanext;

- **Posta elettronica certificata e posta elettronica ordinaria (dati personali e dati particolari)**

- il servizio delle mail aziendali (*nome.cognome@irsm.it*) è stato affidato alla Società Aruba S.p.A. mentre le PEC sono state affidate a Poste Italiane. Le mail del personale vengono eliminate ogni qualvolta il dipendente/consulente cessa di prestare servizio presso l'Istituto;

- **Piattaforma telematica di gestione fornitori**

- ai sensi dell'art 58 D. Lgs. 50/2016 l'Istituto utilizza una propria piattaforma telematica di gestione delle gare e delle trattative dirette, la piattaforma "Net4market" è erogata sull'infrastruttura in Cloud fornita da AWS (Amazon Web Service) nella qualità di hosting provider.

L'accesso ai software sopraelencati avviene con firma elettronica. Le attività svolte vengono registrate e storicizzate consentendo, alle figure autorizzate, il controllo completo della struttura e garantendo una tracciabilità completa dei servizi erogati.

Per quanto afferisce alla gestione dei dati su supporto cartaceo ogni ufficio del San Michele ha la diretta gestione dei propri fascicoli cartacei che vengono conservati in ambienti caratterizzati da accesso riservato a personale dedicato e chiusi con chiave detenuta dai dai singoli operatori competenti.

6. PROCEDURE SPECIFICHE: DATA BREACH, DATA RECOVERY ED ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

6.1 Procedura per il caso di data breach.

Al fine di evitare e contrastare possibili violazioni di dati personali l'Azienda ha previsto una procedura da attivare da parte di ogni Incaricato nel caso in cui venga a conoscenza di una violazione o di una possibile violazione di dati personali trattati dalla Società.

A tal fine l'Azienda ha affidato un ruolo di ricezione delle segnalazioni di *data breach* ad un team di tre soggetti interni, al fine di garantire adeguata copertura sulle medesime.

Il team è composto da: il Responsabile dell'Ufficio ICT, il Responsabile Generale del Trattamento e il Responsabile della protezione dei dati personali.
Ogni Incaricato che dovesse avere conoscenza di una violazione o di una possibile violazione di dati personali trattati dall'Istituto, che si tratti di dati o trattamenti di sua competenza o meno, è tenuto a segnalare immediatamente e comunque entro le 24 ore dal momento dell'avvenuta conoscenza, a mezzo mail all'indirizzo PEO responsabileprotezionedati@irsm.it, le informazioni di cui è a conoscenza.
Il componente del team per il *data breach* che riceve la segnalazione deve, entro il termine massimo di 24 ore dalla stessa, avvertire telefonicamente il Titolare il quale segnalerà l'accaduto:

a) ai membri del sopra citato team nonché ai legali/consulenti esterni privacy dell'Istituto, laddove presenti, affinché possa essere valutata congiuntamente la necessità, secondo quanto previsto dal Regolamento, di procedere alle comunicazioni al Garante ed agli interessati. Nei casi di minore gravità o complessità tale indagine può essere svolta anche in autonomia dal team;
b) in caso di violazione dovuta a problemi agli strumenti informatici o comunque connessa agli stessi, all'Ufficio ICT affinché ne verifichi le cause e interrompa la violazione nel più breve tempo possibile. Quest'ultimo relaziona nel più breve tempo possibile al Titolare sul suo operato e sulle risultanze dell'indagine.

In caso di violazione non dovuta a problemi agli strumenti informatici ma ancora in corso, il team si adopera immediatamente al fine di porre in essere ogni attività necessaria per fermare la violazione, inclusa la richiesta di intervento della autorità di pubblica sicurezza competenti. Il team relaziona nel più breve tempo possibile al Titolare.
In ogni caso nel termine di 72 ore dalla segnalazione, nel caso in cui l'indagine sub a) dia esito positivo l'Azienda invia al Garante la segnalazione contenente i requisiti previsti dall'art 33 del Regolamento. Nel caso in cui dall'indagine emerga la sussistenza dei requisiti di cui all'art. 34 del Regolamento l'Azienda comunica la violazione anche agli interessati, salvo che sia presente una causa di esclusione, senza ritardo.
Il team per il *data breach* è tenuto a redigere un report dettagliato su tutte le attività svolte nel corso della procedura, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, nonché delle comunicazioni effettuate.

6.2 Procedura per data recovery.

Per quanto attiene alle procedure di data recovery dei fornitori di servizi in cloud esse sono state tutte comunicate e acquisite al protocollo dell'Ente (prot. n. 6131/2023).
Per quanto attiene ai dati utilizzati in ambito contabile, custoditi all'interno del database locale ubicato nell'ufficio ragioneria gestito dalla Soc.TP One S.r.l., il server linux (distribuzione ubuntu) ha attualmente 3 metodologie di salvataggio asincrone:

a) copia del disco di backup su salvataggio incrementale con iterazione sugli ultimi 6 mesi (possibilità di fare il ripristino da una qualsiasi data nel periodo indicato);
b) copie compresse con iterazione su ultimi 6 giorni;
c) copia speculare su file sistem.

Le copie sono svolte tramite script di sistema operativo con utente amministratore. La sezione condivisa è inoltre monitorata da software antivirus Claim. Il server è programmato per lo spegnimento automatico a fine salvataggi (ore 22.30) e viene riavviato automaticamente alle ore 7.00 di tutti i giorni.

6.3 Procedura per il caso di esercizio dei diritti degli interessati

L'Istituto ha indicato, quale possibile canale attraverso cui gli interessati possono inviare richieste in merito ai propri diritti relativamente ai dati personali di loro pertinenza trattati dall'Istituto, l'indirizzo di posta elettronica ordinaria responsabileprotezionedati@irsm.it. Il team dedicato, (composto dal Responsabile dell'Ufficio ICT, dal Responsabile Generale del Trattamento e dal Responsabile della protezione dei dati personali), è incaricato di verificare le richieste e le segnalazioni che dovessero pervenire. Entro il termine di 24 ore dal momento in cui viene a conoscenza della richiesta il team dedicato dovrà verificare la sussistenza dei requisiti previsti dal Regolamento per il soddisfacimento della richiesta (ove presenti) e, in caso di esito positivo, dovrà esaudire la richiesta dell'interessato entro le due settimane successive alla ricezione della richiesta (fatta eccezione per l'accesso agli atti il quale seguirà le modalità e le tempistiche dell'apposito regolamento adottato dall'ASP IRSM).

Nel caso in cui non sia possibile, il team dovrà comunicare all'interessato le ragioni dell'impossibilità di soddisfare la sua richiesta.

In particolare il team dovrà:

a) soddisfare tutte le richieste di accesso ai dati e comunicare tutti i dati previsti dall'art. 15 del Regolamento coordinandosi con l'Ufficio competente a gestire gli accessi agli atti documentali nel rispetto della regolamentazione interna all'ASP IRSM afferente alla gestione dell'accesso agli atti documentali;
b) soddisfare tutte le richieste di cancellazione, aggiornamento, rettifica dei dati;
c) soddisfare le richieste di cancellazione solo laddove sussista una delle ragioni di cui al comma 1 dell'art 17 del Regolamento (a titolo esemplificativo, se il trattamento era illegittimo oppure non più necessario o, ancora, basato esclusivamente sul consenso dell'interessato). La cancellazione dovrà essere rifiutata se vi è almeno uno dei motivi di cui al comma 3 del medesimo articolo;
d) soddisfare le richieste di limitazione del trattamento solo laddove ricorra una delle ipotesi di cui all'art. 18 del Regolamento. In tale caso il trattamento sarà limitato soltanto a quanto acconsentito dall'interessato oppure alla difesa/esercizio di un diritto, o per tutelare i diritti di un'altra persona o per motivi di interesse pubblico;
e) soddisfare le richieste di portabilità dei dati, inviando i dati che riguardano l'interessato in formato strutturato di uso comune e leggibile, solo laddove ricorra una delle ipotesi di cui all'art. 20 del Regolamento. Se richiesto e fattibile i dati dovranno essere inviati direttamente al titolare indicato dall'interessato;
f) soddisfare le richieste di opposizione laddove il trattamento sia fondato sul perseguimento di pubblici interessi o del legittimo interesse del titolare salvo che esistano diritti cogenti per proseguire il trattamento che prevalgono sui diritti e le libertà individuali;
g) soddisfare le richieste di opposizione laddove il trattamento sia finalizzato ad attività di marketing diretto;
h) soddisfare le richieste di mancata sottoposizione a trattamenti di profilazione e decisioni automatizzate, nei limiti ed alle condizioni previste dall'art. 22 del Regolamento.

In tutti i casi in cui sia esercitato un diritto previsto tra le lettere a) - d) il team dedicato ha l'obbligo di notificarlo, laddove non sia eccessivamente gravoso, a tutti i soggetti a cui i dati sono stati comunicati.

7. PRESCRIZIONI GENERALI IN MERITO ALLA TUTELA DELLA PRIVACY DI SOGGETTI TERZI

Ciascun Incaricato ha l'obbligo di inviare a mezzo email o consegnare le informative privacy agli interessati con i quali dovesse venire a contatto nel corso della prestazione. In particolare:

- i dipendenti dell'Ufficio Risorse Umane dovranno consegnare il modello di informativa sub all. 1, debitamente compilato, a ciascun nuovo dipendente all'atto dell'assunzione;
- i dipendenti dell'Ufficio Accettazione dovranno consegnare il modello di informativa sub all. 2, a ciascun nuovo ospite, o a un loro referente, della Casa di Riposo e della RSA;
- i dipendenti di ogni ufficio dovranno consegnare il modello di informativa sub all. 3, debitamente compilato, a ciascun nuovo fornitore durante il primo contatto o comunque alla conclusione del contratto.

Sarà responsabilità di ogni singolo ufficio competente per relativa materia somministrare le informative su menzionate. L'Ufficio Internal Audit procederà a svolgere attività di verifica a campione sull'avvenuta somministrazione delle stesse e nel caso in cui dovesse riscontrare che uno o più trattamenti siano effettuati in loro assenza, ovvero di consenso (ove necessario) o oltre il termine previsto dalla policy o dalla relativa informativa, ne darà immediatamente notizia al Responsabile Generale del trattamento, il quale procederà a far cessare immediatamente ogni trattamento non ammesso.

8. PRESCRIZIONI GENERALI IN MERITO ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI

In fase di accensione delle macchine (P.C. e Laptop) ogni dipendente, per poter accedere nel dominio dovrà digitare una password personalizzata. La stessa viene autonomamente scelta dal dipendente e conservata in maniera autonoma.
In seguito alla recente migrazione del server (vedi premessa) sono in fase di programmazione alcune GP (group policy) da impostare una volta ufficializzata la nomina dell'amministratore di sistema, tra le quali il cambio obbligatorio delle password ogni 3 mesi.
Lo stesso procedimento di cui sopra è adottato anche per l'accesso dall'esterno tramite VPN. Ognuno di tali sistemi deve essere dotato di una diversa password.
Le password che saranno impostate dopo l'attivazione delle GP dovranno rispettare i seguenti criteri:

a) avere non meno di 8 caratteri;
b) essere cambiate ogni tre mesi ciascun dipendente;
c) contenere caratteri appartenenti ad almeno tre delle quattro categorie seguenti: caratteri maiuscoli dell'alfabeto inglese (A-Z) - caratteri minuscoli dell'alfabeto inglese (a-z) - cifre decimali (0-9) - caratteri non alfabetici, ad esempio !, $, #, %.

Gli Incaricati non devono mai lasciare incustodito, o accessibile, lo strumento elettronico utilizzato. Inoltre, per evitare possibili intromissioni nelle macchine durante eventuali assenze dall'ufficio nel corso della giornata, sarà prevista l'attivazione automatica, ogni 10 minuti di inattività, dello screen saver, sbloccabile con password personalizzata.
Dopo 5 tentativi di log-in falliti in 15 minuti, l'utenza viene bloccata.
L'utilizzo di Internet e della posta elettronica aziendale deve essere limitato esclusivamente a ricerche e/o attività attinenti alla prestazione lavorativa svolta. Inoltre, la navigazione può essere effettuata solo per scopi consentiti dalla legislazione vigente. Gli utenti sono quindi direttamente responsabili, civilmente e penalmente, per l'uso improprio di Internet e della posta, per la violazione di accessi protetti, per il mancato rispetto delle norme sul copyright e sulle licenze d'uso.

Non è in nessun caso ammesso l'utilizzo di strumenti diversi da quelli forniti dall'azienda per il trattamento di dati personali o comunque per lo svolgimento della prestazione, né in ogni caso il trattamento al di fuori dei limiti della presente policy e del Regolamento.

9. FORMAZIONE

L'istituto prevede annualmente un piano di formazione per tutti i dipendenti con almeno un corso di aggiornamento in materia di diritto della privacy e di applicazione della presente policy. La partecipazione agli eventi formativi è obbligatoria per tutti i dipendenti. La mancata partecipazione ad uno o più eventi formativi senza idonea giustificazione scritta potrà essere disciplinarmente sanzionata.

10. EFFICACIA E AGGIORNAMENTO DELLA POLICY

La presente policy è valida ed efficace sin dalla sua pubblicazione sul sito web istituzionale dell'Istituto Romano di San Michele ed è soggetta ad aggiornamento su base annuale da parte del Titolare.
Una versione della policy viene messa a disposizione di ognuno degli Incaricati all'inizio del rapporto, l'ultima versione disponibile è invece pubblicata all'indirizzo https://www.irsm.it/privacy e, pertanto, ogni Incaricato di cui sopra è tenuto a conoscerla. Per soggetti esterni all'organizzazione aziendale (collaboratori o consulenti) l'ultima versione potrebbe essere resa nota a mezzo dell'indirizzo email utilizzato per lo svolgimento del rapporto. L'eventuale inadempienza rispetto a quanto previsto dalla presente policy da parte dei dipendenti dell'Azienda potrebbe essere considerata disciplinarmente rilevante.
La policy potrà essere aggiornata sia in presenza di innovazioni normative, sia di cambiamenti nell'organizzazione, sia infine con l'obiettivo di migliorare il trattamento dei dati svolto dall'Azienda ed adeguarlo alle novità tecnologiche.
Ogni Incaricato è tenuto a verificare, almeno con cadenza annuale, la pubblicazione di nuove versioni della stessa.

Roma, versione 1.0 pubblicata il 24.08.2023

Istituto Romano di San Michele
Azienda Pubblica di Servizi alla Persona
00147 – Piazzale Antonio Tosti n.4

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PER I DIPENDENTI DELL'ASP ISTITUTO ROMANO DI SAN MICHELE

L'**ASP Istituto Romano di San Michele** (di seguito, per brevità, "**Azienda**" o "**il Titolare**") desidera informarLa, ai sensi della normativa applicabile in materia di protezione dei dati personali, ivi incluso il Regolamento Europeo 679/2016 relativo alla protezione dei dati personali («**Regolamento»**), che i dati personali da Lei forniti in sede di instaurazione del rapporto di lavoro e in costanza di esso, saranno trattati nel rispetto delle disposizioni legislative e contrattuali vigenti per le finalità e con le modalità di seguito indicate. In alcune circostanze alcuni dati potrebbero essere raccolti anche presso terzi, ove necessario e sempre nel rispetto della normativa applicabile.

1. Identità e dati di contatto del Titolare del trattamento, del suo rappresentante e del Responsabile della protezione dei dati

Il Titolare del trattamento è l'Istituto Romano di San Michele, con sede legale in P.le Antonio Tosti n. 4, Roma (di seguito, il «Titolare»), il Rappresentante del Titolare è il Presidente in carica, domiciliato per la carica stessa presso la sede legale del Titolare e il Responsabile della protezione dei dati è stato espressamente nominato con Decreto del Commissario Straordinario, domiciliato per la carica presso la sede del Titolare.

2. Categorie di dati personali, finalità e base giuridica del trattamento

Con riferimento a Lei, l'Azienda tratterà principalmente le seguenti categorie di dati personali:

- **a)** **dati identificativi e di contatto** quali, a titolo di esempio, nome, cognome, data di nascita, codice fiscale, indirizzo, contatti telefonici, residenza, stato civile, stato di famiglia;
- **b)** **dati relativi all'attività lavorativa** quali, a titolo di esempio, incarichi ricoperti, data di assunzione, presenze, numero di matricola, ruolo aziendale, orari e presenze di lavoro, dati relativi alle trasferte, pianificazione attività, altri dati relativi all'attività lavorativa, dati necessari alla partecipazione ad eventi formativi, curriculum lavorativo, dati di *performance*, dati relativi all'anzianità di servizio, retribuzione ed eventuali benefit, permessi, assenze, dati contenuti nelle cartelle di lavoro, valutazioni periodiche;
- **c)** **dati relativi all'instaurazione, gestione e cessazione del rapporto di lavoro** quali, a titolo di esempio, retribuzione, premi, TFR, contributi sociali e assicurativi, estremi del conto corrente bancario, permessi e ferie fruiti e residui, trasferte e trasferimenti ad altre sedi, indennità varie e incentivi;
- **d)** **dati fiscali e reddituali** quali, a titolo di esempio, codice fiscale, cessione del quinto, pignoramenti in essere;
- **e)** **dati previdenziali**;
- **f)** **dati relativi ad eventuali procedimenti di carattere disciplinare ed eventuali procedimenti contenziosi**;
- **g)** **dati acquisiti in relazione all'utilizzo di beni aziendali a Lei concessi in uso**, quali, ad esempio, contravvenzioni al codice della strada, dati relativi all'utilizzo delle carte di credito aziendali, dati relativi ad utenze telefoniche aziendali e dati **relativi alle spese eventualmente sostenute per lo svolgimento delle mansioni**.

I dati personali sopra indicati sono trattati per le seguenti finalità e sulla base delle seguenti condizioni di liceità:

I. adempimento degli obblighi connessi alla gestione del rapporto di lavoro previsti da qualunque disposizione di ogni specie e grado nonché degli obblighi previsti dal CCNL e dagli accordi collettivi applicabili, nonché dal contratto individuale di lavoro; in tale ipotesi la liceità del trattamento si fonda sulla necessità di assolvere gli obblighi legali connessi all'instaurazione e gestione del rapporto di lavoro (art. 6.1, lett. b e c del Regolamento);

II. gestione dell'eventuale contenzioso e tutela dei diritti dell'Azienda; in tale ipotesi la liceità del trattamento si fonda sulla necessità del perseguimento del legittimo interesse dell'Azienda (art. 6.1, lett. f) del Regolamento).

Per tali finalità non occorre il Suo consenso.

Particolari categorie di dati personali ex art. 9 Regolamento: il trattamento di tali dati avrà per oggetto i dati strettamente pertinenti agli obblighi, compiti o finalità connesse alla gestione del rapporto di lavoro e che non possano essere adempiuti o realizzati mediante il trattamento di dati anonimi o di dati personali di natura diversa, i quali possono comprendere i seguenti dati:

- **h)** **dati idonei a rivelare lo stato di salute** (documentazione relativa ad una situazione di invalidità ai fini di un avviamento obbligatorio; certificati di malattia, maternità, infortunio, anche a fini di documentazione delle assenze dal lavoro; referti medici in caso di malattia ai fini del pagamento della relativa indennità; anticipazione del TFR per motivi di salute; dati relativi all'inidoneità al lavoro per l'assegnazione a specifiche mansioni; esposizioni a fattori di rischio; dati concernenti l'inabilità al lavoro ai fini della fruizione dell'assegno per il nucleo familiare; dati per la trasmissione alle compagnie di assicurazione della documentazione medica necessaria per la fruizione dell'assistenza assicurativa della Società in caso di rivalsa);
- **i)** **dati idonei a rivelare l'adesione ad un sindacato** (assunzione di cariche sindacali al fine di fruire di permessi; oppure per la richiesta di trattenuta sullo stipendio per il pagamento di quote associative);
- **j)** **dati idonei a rivelare l'adesione ad un partito politico** (al fine della richiesta di permessi o di aspettative per rivestire cariche pubbliche elettive) o opinioni filosofiche (es. obiezione di coscienza);
- **k)** **dati relativi alla fede religiosa ed alle convinzioni filosofiche** (es. per la fruizione di permessi o festività religiose, per il servizio di mensa, per l'esecuzione di trasferte in Paesi esteri che richiedono tali indicazioni per la concessione del visto, etc.);
- **l)** **dati relativi alla donazione del sangue o all'appartenenza ad associazioni di volontariato** (es. VVF o Protezione civile) ai fini della gestione dei giustificativi di assenza o la richiesta di rimborso a enti pubblici.

In particolare, i Suoi dati relativi alla salute e altre particolari categorie di dati saranno trattati esclusivamente per le seguenti finalità e sulla base delle seguenti condizioni di liceità:

I. per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica. Il trattamento potrebbe anche avere la finalità di salvaguardare la vita o l'incolumità fisica del lavoratore o di un terzo. Per tali finalità non occorre il consenso poiché il trattamento è necessario per eseguire gli obblighi derivanti dal contratto di lavoro e per adempiere agli obblighi previsti dalla legge (art. 6.1, lett. b e c del Regolamento) o della specifica ipotesi di salvaguardia dell'incolumità fisica dell'interessato o di un terzo (Regolamento art 6.1, lett. d). In tali casi il trattamento è fondato sulle condizioni di liceità di cui all'art. 9.2, lett. b, c e h, rispettivamente connesse alla necessità di assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, necessità di tutelare un interesse vitale dell'interessato e a finalità di medicina preventiva e del lavoro.

Alcuni dei dati di cui sopra (a titolo esemplificativo, status maritale, carichi familiari e quant'altro) potrebbero essere relativi anche a componenti del Suo nucleo familiare. Nel momento in cui ci comunicherà tali dati Lei dichiara, sotto la propria responsabilità, di aver mostrato i contenuti della presente informativi agli interessati e che gli stessi sono stati compresi e accettati.

3. Modalità del trattamento e natura del conferimento

I dati personali saranno trattati dall'Azienda con sistemi informatici e cartacei secondo i principi di correttezza, lealtà e trasparenza previsti dalla normativa applicabile in materia di protezione dei dati personali e tutelando la Sua riservatezza e i Suoi diritti mediante l'adozione d'idonee misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio.

Il conferimento e l'aggiornamento dei Suoi dati personali è obbligatorio in base a normative vigenti (in materia fiscale, assistenziale, previdenziale, a tutela della salute dei lavoratori sui luoghi di lavoro o altre) o per lo svolgimento del rapporto di lavoro. Il conferimento di alcuni dati richiesti è obbligatorio per l'adempimento di prestazioni o la concessione di benefici in Suo favore (ad es. i carichi familiari). Senza tali dati, non sarà possibile instaurare o - in talune circostanze - proseguire il rapporto di lavoro o comunque dar corso alle Sue richieste o comunque ai benefici per i quali tali dati sono richiesti e comunicati.

4. Conservazione dei dati

Tutti i dati a Lei riferibili saranno conservati nel rispetto degli obblighi civilistici e fiscali (ad esempio obbligo civilistico di conservare le scritture contabili e ulteriore corrispondenza aziendale per 10 anni). La maggior parte dei dati di cui sopra sarà conservata per tutto il Suo rapporto di lavoro. Una volta concluso il rapporto di lavoro, a tutela dei diritti dell'Azienda, i dati saranno conservati – in modo da essere accessibili solo in caso di necessità – per un periodo di tempo corrispondente al periodo di prescrizione di eventuali diritti che Lei possa vantare nei confronti dell'Azienda. Tale periodo varia a seconda del tipo di dato e dell'eventuale intervento di cause interruttive o sospensive della prescrizione medesima.

5. Destinatari dei dati

I Suoi dati non saranno oggetto di diffusione ma, per le finalità sopra indicate e nel rispetto dei principi del Regolamento, potranno essere comunicati a: altri dipendenti dell'Azienda, i suoi collaboratori, consulenti e professionisti (in particolare, a mero titolo esemplificativo: medico competente; commercialisti e studi paghe incaricati; avvocati). Nell'adempimento di obblighi di legge, di quelli derivanti dal rapporto di lavoro o su Sua richiesta, i dati potrebbero essere comunicati a enti pubblici, pubblica autorità, fondi o casse di previdenza, istituti di credito, Suoi familiari o affini, ove strettamente necessario alla Sua salvaguardia.

6. Trasferimento dei dati

I Suoi dati, ad esclusione di quelli contenuti nell'art. 2 lettere c) della presente informativa, saranno conservati presso il server aziendale posto all'interno del CED (Centro elaborazione dati) al piano terra della palazzina "Uffici" gestito da personale autorizzato, il quale provvede a vigilare sulla corretta esecuzione dei backup giornalieri, eseguiti su apposita NAS (Network Attached Storage) posizionata all'interno di un armadietto Rec allocato in diversa stanza rispetto al CED e ubicato nel piano primo della palazzina "Uffici".

I dati contenuti nell'art. 2 lettera c), sono custoditi in parte nel database locale ubicato all'interno dell'ufficio ragioneria gestito dalla Soc. TP One S.r.l. - appositamente nominata "Responsabile esterno del trattamento" - che ne cura e coordina i backup sia su server locale che su server Cloud ed in parte dalla Società Wolters Kluwer Italia S.r.l. - appositamente nominata "Responsabile esterno del trattamento" - che gestisce e conserva dati con i relativi backup su server Cloud sulla base di un contratto di servizi con il Titolare.

I dati sensibili (es. certificati di malattia, infortuni, esiti tamponi) che transitano presso il software del protocollo informatico dell'Ente, sono gestiti dalla Società Dedagroup S.p.A. - appositamente nominata "Responsabile esterno del trattamento" - attraverso la suite Civilia Next, la quale si appoggia su piattaforma di cloud computing Microsoft Azure, conforme alla normativa sulla privacy contenuta nel modello UE.

7. Diritti dell'interessato

L'interessato potrà esercitare, in relazione al trattamento dei dati ivi descritto, i diritti previsti dalla normativa applicabile in materia di protezione dei dati personali, ivi incluso il diritto di:

- ricevere conferma dell'esistenza dei suoi dati personali e accedere al loro contenuto (diritti di accesso);
- aggiornare, modificare e/o correggere i suoi dati personali (diritto di rettifica);
- chiederne la cancellazione o la limitazione del trattamento dei dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o altrimenti trattati (diritto all'oblio e diritto alla limitazione);
- opporsi al trattamento fondato sul legittimo interesse (diritto di opposizione);
- revocare il consenso, ove prestato, senza pregiudizio per la liceità del trattamento basata sul consenso precedentemente prestato;
- proporre reclamo all'Autorità di controllo in caso di violazione della disciplina in materia di protezione dei dati personali;
- ricevere copia dei dati in formato elettronico che lo riguardano resi nel contesto del contratto di lavoro (es. dati relativi agli stipendi, servizi di mobilità interni) e chiedere che tali dati siano trasmessi ad un altro titolare del trattamento (diritto alla portabilità dei dati).

Per esercitare tali diritti può rivolgersi in qualsiasi momento al Titolare, inviando la Sua richiesta al seguente indirizzo email *responsabileprotezionedati@irsm.it* o mediante raccomandata a/r al seguente indirizzo: P.le Antonio Tosti n. 4, Roma.

Il/la sottoscritto/a _____ dichiara di avere preso visione e letto in ogni sua parte la sopra estesa informativa di cui all'art. 13 del Regolamento Europeo 679/2016.

Luogo _____ Data _____ Firma dell'interessato/a _____

Istituto Romano di San Michele
Azienda Pubblica di Servizi alla Persona
00147 – Piazzale Antonio Tosti n.4

INFORMATIVA PER CLIENTI/OSPITI CASA DI RIPOSO ed RSA

L'ASP Istituto Romano di San Michele (di seguito, per brevità, "**Azienda**" o "**il Titolare**"), in qualità di titolare del trattamento desidera informarLa, ai sensi della normativa applicabile in materia di protezione dei dati personali, ivi incluso il Regolamento Europeo 679/2016 relativo alla protezione dei dati personali («**Regolamento»**), che i dati personali da Lei forniti in sede di instaurazione del rapporto e in costanza di esso, saranno trattati nel rispetto delle disposizioni legislative e contrattuali vigenti per le finalità e con le modalità di seguito indicate. In alcune circostanze alcuni dati potrebbero essere raccolti anche presso terzi, ove necessario e sempre nel rispetto della normativa applicabile.

1. Identità e dati di contatto del Titolare del trattamento, del suo rappresentante e del Responsabile della protezione dei dati

Il Titolare del trattamento è l'ASP Istituto Romano di San Michele, con sede legale in P.le Antonio Tosti n. 4 - Roma, il Rappresentate del Titolare è il Presidente in carica, domiciliato per la carica presso la sede legale del Titolare. Il Responsabile della protezione dei dati è stato espressamente nominato con Decreto del Commissario Straordinario, domiciliato per la carica presso la sede legale del Titolare, indirizzo email *responsabileprotezionedati@irsm.it* (di seguito, il «**Responsabile**»).

2. Categorie di dati personali, finalità e base giuridica del trattamento

Il Titolare potrà trattare:

- **dati identificativi e di contatto**: nome e cognome o ragione sociale, codice fiscale o partita IVA, residenza o sede legale, indirizzo email, numero telefonico;
- **dati di natura fiscale o comunque necessari per eseguire o ricevere pagamenti**.

I dati personali sopra indicati sono trattati per le seguenti finalità e sulla base delle seguenti condizioni di liceità:

1. adempiere agli obblighi derivanti dalla legge e/o dal rapporto in essere con il Titolare, cui la presente informativa è allegata, e comunque di fornire le attività di consulenza e assistenza richieste; in tale ipotesi la liceità del trattamento si fonda sulla necessità di assolvere gli obblighi legali connessi all'instaurazione e gestione del rapporto contrattuale (art. 6.1, lett. b e c del Regolamento);

2. gestione dell'eventuale contenzioso e tutela dei diritti dell'Azienda; in tale ipotesi la liceità del trattamento si fonda sulla necessità del perseguimento del legittimo interesse dell'Azienda (art. 6.1, lett. f del Regolamento).
Per tali finalità non occorre il Suo consenso.

3. Modalità del trattamento e natura del conferimento
I dati personali saranno trattati dall'Azienda con sistemi informatici e cartacei secondo i principi di correttezza, lealtà e trasparenza previsti dalla normativa applicabile in materia di protezione dei dati personali e tutelando la Sua riservatezza e i Suoi diritti mediante l'adozione d'idonee misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio.

Il conferimento e l'aggiornamento dei Suoi dati personali è obbligatorio in base a normative vigenti (in materia fiscale o altre) o per lo svolgimento del rapporto contrattuale. Senza tali dati, non sarà possibile instaurare o - in talune circostanze - proseguire il rapporto.

4. Conservazione dei dati
Tutti i dati a Lei riferibili saranno conservati nel rispetto degli obblighi civilistici e fiscali (ad esempio obbligo civilistico di conservare le scritture contabili e ulteriore corrispondenza aziendale per 10 anni) e comunque per la sola durata del contratto in essere. Una volta concluso il rapporto, a tutela dei diritti dell'Azienda, i dati saranno conservati – in modo da essere accessibili solo in caso di necessità – per un periodo di tempo corrispondente al periodo di prescrizione di eventuali diritti che Lei possa vantare nei confronti dell'Azienda. Tale periodo varia a seconda del tipo di dato e dell'eventuale intervento di cause interruttive o sospensive della prescrizione medesima.

5. Destinatari dei dati
I Suoi dati non saranno oggetto di diffusione ma, per le finalità sopra indicate e nel rispetto dei principi del Regolamento, potranno essere comunicati a: dipendenti dell'Azienda, i suoi collaboratori, consulenti e professionisti (in particolare, a mero titolo esemplificativo: commercialisti; gestore del database aziendale etc.). Nell'adempimento di obblighi di legge, di quelli derivanti dal rapporto contrattuale o su Sua richiesta, i dati potrebbero essere comunicati a enti pubblici, o alla pubblica autorità.

6. Trasferimento dei dati

I Suoi dati saranno conservati presso il server aziendale posto all'interno del CED (Centro elaborazione dati) al piano terra della palazzina "Uffici" gestito da personale autorizzato, il quale provvede a vigilare sulla corretta esecuzione dei backup giornalieri, eseguiti su apposita NAS (Network Attached Storage) posizionata all'interno di un armadietto Rec allocato in diversa stanza rispetto al CED e ubicato nel piano primo della palazzina "Uffici".

Alcuni dati (es. estremi conto corrente bancario); sono custoditi in parte nel database locale ubicato all'interno dell'ufficio ragioneria gestito dalla Soc. TP One S.r.l. - appositamente nominata "Responsabile esterno del trattamento" - che ne cura e coordina i backup sia su server locale che su server Cloud ed in parte dalla Società Wolters Kluwer Italia S.r.l. - appositamente nominata "Responsabile esterno del trattamento" - che gestisce e conserva dati con i relativi backup su server Cloud sulla base di un contratto di servizi con il Titolare.

I dati sensibili che transitano presso il software del protocollo informatico dell'Ente, sono gestiti dalla Società Dedagroup S.p.A. - appositamente nominata "Responsabile esterno del trattamento" - attraverso la suite Civilia Next, la quale si appoggia su piattaforma di cloud computing Microsoft Azure, conforme alla normativa sulla privacy contenuta nel modello UE.

7. Diritti dell'interessato

L'interessato potrà esercitare, in relazione al trattamento dei dati ivi descritto, i diritti previsti dalla normativa applicabile in materia di protezione dei dati personali, ivi incluso il diritto di:

- ricevere conferma dell'esistenza dei suoi dati personali e accedere al loro contenuto (diritto di accesso);
- aggiornare, modificare e/o correggere i suoi dati personali (diritto di rettifica);
- chiederne la cancellazione o la limitazione del trattamento dei dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o altrimenti trattati (diritto all'oblio e diritto alla limitazione);
- opporsi al trattamento fondato sul legittimo interesse (diritto di opposizione);
- revocare il consenso, ove prestato, senza pregiudizio per la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo all'Autorità di controllo in caso di violazione della disciplina in materia di protezione dei dati personali;
- ricevere copia dei dati in formato elettronico che lo riguardano resi nel contesto del contratto di lavoro (es. dati relativi agli stipendi, servizi di mobilità interni) e chiedere che tali dati siano trasmessi ad un altro titolare del trattamento (diritto alla portabilità dei dati).

Per esercitare tali diritti può rivolgersi in qualsiasi momento al Responsabile per la protezione dei dati, inviando la Sua richiesta al seguente indirizzo email *responsabileprotezionedati@irsm.it* o mediante raccomandata a/r al seguente indirizzo: P.le Antonio Tosti, 4.

Il/la sottoscritto/a _____ dichiara di avere preso visione e letto in ogni sua parte la sopra estesa informativa di cui all'art. 13 del Regolamento Europeo 679/2016.

Luogo _____ Data _____Firma dell'interessato _____

Istituto Romano di San Michele
Azienda Pubblica di Servizi alla Persona
00147 – Piazzale Antonio Tosti n.4

INFORMATIVA PER I FORNITORI

L'ASP Istituto Romano di San Michele (di seguito, per brevità, "**Azienda**" o "**il Titolare**"), in qualità di titolare del trattamento desidera informarLa, ai sensi della normativa applicabile in materia di protezione dei dati personali, ivi incluso il Regolamento Europeo 679/2016 relativo alla protezione dei dati personali («**Regolamento»**), che i dati personali da Lei forniti in sede di instaurazione del rapporto e in costanza di esso, saranno trattati nel rispetto delle disposizioni legislative e contrattuali vigenti per le finalità e con le modalità di seguito indicate. In alcune circostanze alcuni dati potrebbero essere raccolti anche presso terzi, ove necessario e sempre nel rispetto della normativa applicabile.

1. Identità e dati di contatto del Titolare del trattamento e del suo rappresentante e del Responsabile della protezione dei dati

Il Titolare del trattamento è l'Istituto Romano di San Michele, con sede legale in P.le Antonio Tosti n. 4 - Roma, il Rappresentate del Titolare è il Presidente in carica, domiciliato per la carica presso la sede legale del Titolare. Il Responsabile della protezione dei dati è espressamente nominato con Decreto del Commissario Straordinario, domiciliato per la carica presso la sede legale del Titolare, indirizzo e-mail *responsabileprotezionedati@irsm.it* (di seguito, il «**Responsabile**»).

2. Categorie di dati personali, finalità e base giuridica del trattamento

Il Titolare potrà trattare:

- **dati identificativi e di contatto**: nome e cognome o ragione sociale, codice fiscale o partita IVA, residenza o sede legale, indirizzo email, numero telefonico;
- **dati di natura fiscale o comunque necessari per eseguire o ricevere pagamenti**.

I dati personali sopra indicati sono trattati per le seguenti finalità e sulla base delle seguenti condizioni di liceità:

1. adempiere agli obblighi derivanti dalla legge e/o dal contratto in essere con il Titolare, cui la presente informativa è allegata; in tale ipotesi la liceità del trattamento si fonda sulla necessità di assolvere gli obblighi legali connessi all'instaurazione e gestione del rapporto contrattuale (art. 6.1, lett. b e c del Regolamento);

2. gestione dell'eventuale contenzioso e tutela dei diritti della Società; in tale ipotesi la liceità del trattamento si fonda sulla necessità del perseguimento del legittimo interesse della Società (art. 6.1, lett. f del Regolamento).
Per tali finalità non occorre il Suo consenso.

3. Modalità del trattamento e natura del conferimento
I dati personali saranno trattati dall'Azienda con sistemi informatici e cartacei secondo i principi di correttezza, lealtà e trasparenza previsti dalla normativa applicabile in materia di protezione dei dati personali e tutelando la Sua riservatezza e i Suoi diritti mediante l'adozione d'idonee misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio.

Il conferimento e l'aggiornamento dei Suoi dati personali è obbligatorio in base a normative vigenti (in materia fiscale o altre) o per lo svolgimento del rapporto contrattuale. Senza tali dati, non sarà possibile instaurare o - in talune circostanze - proseguire il rapporto.

4. Destinatari dei dati
I Suoi dati non saranno oggetto di diffusione ma, per le finalità sopra indicate e nel rispetto dei principi del Regolamento, potranno essere comunicati a: dipendenti dell'Azienda, i suoi collaboratori, consulenti e professionisti (es. commercialisti). Nell'adempimento di obblighi di legge, di quelli derivanti dal rapporto contrattuale o su Sua richiesta di dati potrebbero essere comunicate a enti pubblici, o alla pubblica autorità.

5. Conservazione e Trasferimento dei dati

Tutti i dati a Lei riferibili saranno conservati nel rispetto degli obblighi civilistici e fiscali (ad esempio obbligo civilistico di conservare le scritture contabili e ulteriore corrispondenza aziendale per 10 anni) e comunque per la sola durata del contratto in essere. Una volta concluso il rapporto, a tutela dei diritti dell'Azienda, i dati saranno conservati – in modo da essere accessibili solo in caso di necessità – per un periodo di tempo corrispondente al periodo di prescrizione di eventuali diritti che Lei possa vantare nei confronti della Società. Tale periodo varia a seconda del tipo di dato e dell'eventuale intervento di cause interruttive o sospensive della prescrizione medesima.

I Suoi dati saranno conservati presso il server aziendale posto all'interno del CED (Centro elaborazione dati) al piano terra della palazzina "Uffici" gestito da personale autorizzato, il quale provvede a vigilare sulla corretta esecuzione dei backup giornalieri, eseguiti su apposita NAS (Network Attached Storage) posizionata all'interno di un armadietto Rec allocato in diversa stanza rispetto al CED e ubicato nel piano primo della palazzina "Uffici".

Alcuni dati (es. estremi conto corrente bancario)~~,~~ sono custoditi in parte nel database locale ubicato all'interno dell'ufficio ragioneria gestito dalla Soc. TP One S.r.l. - appositamente nominata "Responsabile esterno del trattamento" - che ne cura e coordina i backup sia su server locale che su server Cloud ed in parte dalla Società Wolters Kluwer Italia S.r.l. - appositamente nominata "Responsabile esterno del trattamento" - che gestisce e conserva dati con i relativi backup su server Cloud sulla base di un contratto di servizi con il Titolare.

I dati che transitano presso il software del protocollo informatico dell'Ente, sono gestiti dalla Società Dedagroup S.p.A. - appositamente nominata "Responsabile esterno del trattamento" - attraverso la suite Civilia Next, la quale si appoggia su piattaforma di cloud computing Microsoft Azure, conforme alla normativa sulla privacy contenuta nel modello UE.

I dati che transitano sulla piattaforma adibita alla registrazione\iscrizione dei fornitori gestita dalla Soc.Net4market, – CSAmed s.r.l., è qualificata al Cloud Marketplace di AgID per i servizi SAAS ed erogata su un'infrastruttura già attiva, collaudata, stabile e sicura all'interno del proprio cloud privato (VPC – Virtual Private Network) ospitato presso AWS (Amazon Web Services), CSP (Cloud Service Provider) qualificato al Cloud Marketplace di AgID per i servizi IAAS. Il sito primario è presso il datacenter di Parigi, mentre il sito secondario (disaster recovery) è presso il datacenter di Francoforte. I dati personali trattati dalla piattaforma sono cifrati e presenti sul database in via pseudonimizzata, nonché quotidianamente backuppati in modo da garantire l'eventuale ripristino.

6. Diritti dell'interessato

L'interessato potrà esercitare, in relazione al trattamento dei dati ivi descritto, i diritti previsti dalla normativa applicabile in materia di protezione dei dati personali, ivi incluso il diritto di:

- ricevere conferma dell'esistenza dei suoi dati personali e accedere al loro contenuto (diritti di accesso);
- aggiornare, modificare e/o correggere i suoi dati personali (diritto di rettifica);
- chiederne la cancellazione o la limitazione del trattamento dei dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o altrimenti trattati (diritto all'oblio e diritto alla limitazione);
- opporsi al trattamento fondato sul legittimo interesse (diritto di opposizione);
- revocare il consenso, ove prestato, senza pregiudizio per la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo all'Autorità di controllo in caso di violazione della disciplina in materia di protezione dei dati personali;
- ricevere copia dei dati in formato elettronico che lo riguardano resi nel contesto del contratto di lavoro (es. dati relativi agli stipendi, servizi di mobilità interni) e chiedere che tali dati siano trasmessi ad un altro titolare del trattamento (diritto alla portabilità dei dati).

Per esercitare tali diritti può rivolgersi in qualsiasi momento al Responsabile per la protezione dei dati, inviando la Sua richiesta al seguente indirizzo email *responsabileprotezionedati@irsm.it* o mediante raccomandata a/r al seguente indirizzo: P.le Antonio Tosti n. 4, Roma.

Il/la sottoscritto/a _____ dichiara di avere preso visione e letto in ogni sua parte la sopra estesa informativa di cui all'art. 13 del Regolamento Europeo 679/2016.

Luogo _____ Data _____ Firma dell'interessato _____