HOSPITALIA SRL
RSA Rosolina
Via Marangon 10, 45010 Rosolina (RO)
Codice fiscale e Partita IVA 09491140969

MANUALE PRIVACY

Redatto in base alle disposizioni del

REGOLAMENTO UE N. 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
DEL 27 APRILE 2016 (in seguito, "GDPR")
e del
DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196
AGGIORNATO AL DECRETO LEGISLATIVO 10 AGOSTO 2018, N. 101

1. ELENCO DELLE REVISIONI

n. Revisione	Data	Oggetto della revisione	Verifica e approvazione del Titolare del trattamento / Legale Rappresentante
00	01/02/2020	Prima edizione	Sergio Annoscia

Sommario

2. GENERALITA’

2.1. Scopo

Lo scopo del presente Manuale è di delineare il quadro delle misure adeguate di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali comuni, particolari o giudiziari, in conformità allo spirito ed ai principi generali espressi dal Regolamento EU 2016/679 (nel seguito GDPR), nonché secondo le esigenze di gestione dei rischi aziendali.

Sono identificabili i seguenti obiettivi particolari perseguiti nello sviluppo e nella redazione aggiornata del Manuale:

- identificare i trattamenti di dati personali effettuati in azienda
- identificare le classi omogenee di incaricati, o i singoli incaricati laddove necessario, e i relativi profili di autorizzazione ai trattamenti (operazioni di trattamento consentite);
- analizzare i rischi connessi con il trattamento dei dati;
- definire e regolamentare le più adeguate misure di sicurezza che devono essere adottate per garantire la sicurezza dei dati in termini di integrità, disponibilità, riservatezza e trattamento conforme alle finalità, riducendo al minimo i rischi che incombono sui dati;
- stabilire le modalità di comunicazione, informazione e formazione
- stabilire la pianificazione generale di ogni scelta inerente alla sicurezza dei dati personali trattati dall'azienda; in particolare per i trattamenti meno standard o più a rischio implementare i principi di privacy by design e by default nella loro mappatura.

2.2. Campo di applicazione

2.2.1. Trattamenti di dati personali

Il presente Manuale prevede l'identificazione e l'analisi dei rischi riguardanti i seguenti ambiti di trattamento di dati personali individuati:

- dati personali, comuni, relativi ai dipendenti, nell'ambito del rapporto di collaborazione;
- dati personali, comuni, particolari e giudiziari, relativi agli ospiti, nell'ambito del rapporto contrattuale di erogazione dei servizi;
- dati personali, comuni, particolari e giudiziari, relativi ai clienti, nell'ambito del rapporto contrattuale di erogazione dei servizi;
- dati personali relativi ai Fornitori, nell'ambito del rapporto contrattuale di fornitura;
- dati personali (immagini) relativi a persone fisiche (ospiti, visitatori, fornitori, ecc) relativamente al sistema di videosorveglianza.

Il campo di applicazione del presente Manuale è costituito quindi complessivamente dai trattamenti di dati personali:

- particolari, giudiziari, personali comuni;
- effettuati sia con l'ausilio di strumenti elettronici sia senza l'ausilio di strumenti elettronici;
- effettuati sia internamente all'azienda che affidati a strutture esterne (outsourcing).

Per tutte le categorie di dati personali trattate in azienda, vengono comunque definite le regole generali e gli adempimenti richiesti dal Regolamento GDPR 2016/679 e dalle linee guida e provvedimenti del Garante, per assicurare l'adozione delle misure minime e degli altri adempimenti di legge sulla sicurezza. Vengono inoltre stabilite procedure di gestione della sicurezza, per contrastare rischi di carattere generale inerenti a tutte le categorie di dati personali.

2.3. Riferimenti

2.3.1. Riferimenti legislativi

N.	Codice	Titolo	Edizione
[1]	GDPR UE 679/2016	Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE	27/04/2016
[2]	Provvedimento n. 523 Garante per la Protezione dei Dati Personali	Autorizzazione n. 1/2016 - Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro - 15 dicembre 2016 (Pubblicato sulla Gazzetta Ufficiale n. 303 del 29 dicembre 2016)	15/12/2016
[3]	Provvedimento n. 229 Garante per la Protezione dei Dati Personali	Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - (Pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014)	08/05/2014
[4]	D.Lgs 2012	Art. 45 Semplificazioni in materia di dati personali - Decreto-legge 9 febbraio 2012, n. 5 Recante disposizioni urgenti in materia di semplificazione e di sviluppo, convertito con modificazioni, dalla legge 4 aprile 2012, n. 35 (Gazzetta Ufficiale n. 82 del 6 aprile 2012)	9/02/2012
[5]	Provvedimento in materia di videosorveglianza Garante per la Protezione dei Dati Personali	Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Gazzetta Ufficiale n. 99 del 29 aprile 2010)	08/04/2010
[6]	Provvedimento n. 229 Garante per la Protezione dei Dati Personali	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) - così modificato in base al provvedimento del 25 giugno 2009	27/11/2008 12/02/2009
[7]	Decreto legislativo 30 giugno 2003, n. 196 Aggiornato al Decreto Legislativo 10 agosto 2018, n. 101	CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE	10/08/2018

2.4. Termini e definizioni

Archivio

Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca di dati (v. archivio)

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Classi omogenee di incaricati

Gruppo definito di incaricati a cui è consentito in modo omogeneo un insieme stabilito di trattamenti.

Classi omogenee di incarico

Insieme di operazioni effettuate da un gruppo definito di incaricati.

Consenso

Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Credenziali di autenticazione

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Dati identificativi

I dati personali che permettono l'identificazione diretta dell'interessato.

Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Dati personali

Qualsiasi informazione riguardante una persona fisica persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con un particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari

Ex dati sensibili: I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere

religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dato genetico

I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute dei detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione

Dati biometrici

I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dato salute

I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Dati che presentano rischi

Es: profilazione, geolocalizzazione, biometrici, registrazioni audio e video…

Destinatario

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Gruppo imprenditoriale

Un gruppo costituito da un'imprese controllante e dalle imprese da questa controllate.

Impresa

La persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

Incaricati (v. responsabile trattamento)

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato

La persona fisica cui si riferiscono i dati personali.

Limitazione - Trattamento dati

Contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

Profilazione

Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessati, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Pseudonomizzazione

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Rappresentante

La persona fisica o la persona giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

Responsabile trattamento

La persona fisica, la persona giuridica, la pubblica amministrazione, l'autorità pubblica e qualsiasi altro ente, associazione od organismo che tratti dati personali per conto del titolare al trattamento.

Rischi generali

Eventi incerto o un insieme di eventi che, se si verificassero, potrebbero avere un effetto sulla protezione dei dati personali, che possono essere suddivisibili in: rischi legati al comportamento delle persone; rischi relativi agli strumenti di lavoro; rischi relativi al contesto in cui si opera.

Gli eventi incerti possono essere legati a:

- indisponibilità dei processi, ovvero i processi non esistono più o non funzionano più;
- accesso illegittimo ai dati personali da parte di persone non autorizzate;
- alterazioni, modifiche o distruzioni accidentali dei dati personali;
- indisponibilità dei dati personali;
- trattamento difforme da quello inizialmente previsto (deviazione dalla finalità definita, eccessiva o scorretta raccolta dei dati …).

Stabilimento principale

Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale.

Con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.

Sicurezza del trattamento (v. Misure adeguate)

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che - tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche - il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Sistema di autorizzazione

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Terze parti

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Titolare trattamento

La persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati Membri, il titolare del trattamento o i criteri applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati Membri.

Trattamento dati

Qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione, anche se non registrati in una banca di dati.

Violazione

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.

2.4.1. Modalità di gestione, modifica e aggiornamento del documento

Il Manuale viene redatto e aggiornato dal Titolare del trattamento che ne garantisce:

- la comunicazione agli incaricati aziendali che garantiranno l'applicazione dei contenuti
- la valutazione della necessità di modifica e di aggiornamento ogni qualvolta siano effettuate variazioni aziendali in termini organizzativi, strutturali del sito aziendale, tecnici, tecnologici, contrattuali, procedurali, di trattamento relativo a dati personali che abbiano influenza sulla sicurezza dei dati personali.

A tale scopo il Titolare del trattamento organizza e coordina riesami periodici con le funzioni aziendali pertinenti finalizzati alla individuazione delle eventuali variazioni intervenute, quando queste non siano state precedentemente a lui comunicate dalle stesse funzioni.

Pur rimanendo incaricato della conduzione del sistema per la sicurezza dei dati personali, il Titolare del trattamento può avvalersi del supporto di consulenti esterni esperti nel settore per effettuare le attività operative sopra descritte.

2.4.2. Distribuzione e riservatezza

Il Manuale viene messo a disposizione degli incaricati aziendali dal Titolare del trattamento in formato elettronico (cartella del Server aziendale) ed è un documento interno riservato che non può essere diffuso in alcuna forma all'esterno dell'azienda, fatti salvi i casi descritti più avanti nel presente paragrafo.

Tale vincolo è esteso a tutti i documenti che definiscono e documentano le misure di sicurezza ai fini della protezione dei dati personali, fatti salvi i casi in cui le stesse misure ne prevedano l'impiego non riservato.

Tuttavia il Manuale viene messo a disposizione di Enti esterni di controllo (Garante per la protezione dei dati personali, Guardia di Finanza, Polizia Postale, Organismo di Vigilanza legge 231, Auditor Interni, o altri Enti preposti ai controlli in materia di sicurezza dei dati personali) a fronte di richieste motivate o di esigenze cogenti per la consultazione.

A fronte di esigenze specifiche e circoscritte di regolamentazione del trattamento dei dati personali, il Titolare del trattamento può decidere l'estrazione di parti del Manuale e la loro comunicazione a: Personale interno, Clienti, Fornitori o altri Enti esterni, in base a quanto di volta in volta pertinente.

3. CONTESTO DELL'AZIENDA E DEI DATI TRATTATI

HOSPITALIA SRL è l'ente gestore della RSA (Residenza Sanitaria Assistenziale) avente sede a Rosolina in provincia di Rovigo. La Residenza è in regime di accreditamento ASL della Regione Veneto.

L'accoglimento della persona non autosufficiente nelle Residenze della Regione Veneto è regolamentato da Leggi Regionali che hanno stabilito l'iter per la domanda. La persona non autosufficiente verrà inserita nella Lista Unica per l'accesso ai servizi residenziali e verrà contattata dalle Residenze prescelte quando sarà prima nella loro graduatoria. L'attivazione della convenzione è subordinata all'emissione da parte dell'Azienda Ulss competente dell'Impegnativa di Residenzialità su richiesta della Residenza proponente.

La RSA di Rosolina si trova in Via Marangon 10 e presso questa sede si svolgono le principali attività di trattamento.

La RSA di Rosolina, oltre che del proprio personale amministrativo, si avvale di competenze specifiche in ambito medico/infermieristico che vengono fornite dalla UNIVERSIIS – SOCIETA' COOPERATIVA SOCIALE, erogate sulla base del contratto stipulato e che è stata nominata Responsabile del Trattamento dei dati.

Non vengono svolte attività di profilazione. I dati aggregati resi anonimi possono essere elaborati esclusivamente a fini statistici interni.

In base alla tipologia di attività, di relazioni esistenti con l'esterno e di risorse impiegate, le categorie di dati personali trattati in azienda sono quelli indicati al punto 2.2.1 del presente Manuale.

4. POLITICA GENERALE PER LA SICUREZZA DEI DATI PERSONALI

4.1. Principi generali per la sicurezza dei dati personali trattati

Indipendentemente dall'obbligo di rispettare le misure generali e specifiche stabilite nei paragrafi successivi, chiunque in azienda tratti dati personali, inclusi i responsabili delle funzioni nelle quali sono effettuate operazioni di trattamento, è tenuto all'applicazione dei seguenti principi generali dei quali deve essere dato riscontro nell'operatività delle strutture interessate.

4.2. Criteri generali di trattamento dei dati

Nella scelta, definizione ed attuazione delle operazioni di trattamento dei dati personali (siano essi trattati con o senza l'ausilio di strumenti elettronici), occorre assicurare che tali dati siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati e dalla perdita, distruzione e danno accidentali, mediante misure tecniche e organizzative adeguate.

5. ORGANIZZAZIONE PER LA SICUREZZA DEI DATI PERSONALI

5.1. Organigramma aziendale per la sicurezza

Il Titolare del trattamento è HOSPITALIA SRL, Rappresentata dal Presidente Sergio Annoscia.

5.2. Il Responsabile Protezione Dati (RPD)

L'art. 37 del Regolamento UE 2016/679 stabilisce i requisiti relativi all'obbligo di nomina del RPD, che deve essere sistematicamente designato ogniqualvolta:

a) Il trattamento è effettuato da un'autorità pubblica;
b) Le attività principali del titolare del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) Le attività principali del titolare del trattamento consistono nel trattamento su larga scala di dati particolari o relativi a condanne penali e reati.

HOSPITALIA SRL rientra nella casistica definita al punto c) in quanto effettua trattamento di dati particolari tipici dell'attività svolta dalle RSA. Il trattamento è limitato agli ospiti della RSA di Rosolina, il cui numero non è associabile alla larga scala. La direzione ha stabilito di avvalersi di un RPD quale misura ulteriore di protezione dei dati.

Previa verifica del possesso di adeguate competenze e idonei requisiti nel rispetto delle Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016 è stata nominata RPD la sig.ra Radice Paola, consulente libera professionista, avente sede in Via Adamoli 12 a Varese, codice fiscale RDCPLA69S45E734R.

5.3. Responsabilità per la sicurezza

Le responsabilità relative alla sicurezza dei dati personali vengono integrate con quelle stabilite in modo più generale dall'organizzazione aziendale e vengono definite secondo quanto descritto nei paragrafi che seguono.

5.3.1. Titolare del trattamento

- ha le responsabilità e le autorità stabilite dal GDPR 2016/679 per il Titolare del trattamento dei dati personali;
- in assenza del RPD è l'interlocutore del Garante. Ha le prerogative di accountability come definite dal GDPR 2016/679
- tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Provvede a riesaminare e aggiornare dette misure qualora necessario
- ha facoltà di designare uno o più responsabili del trattamento, individuandolo/i tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- specifica analiticamente per iscritto i compiti affidati al responsabile;
- fornisce al responsabile del trattamento le politiche e le direttive generali in merito al trattamento dei dati personali ad al profilo di sicurezza da garantire;
- effettua l'approvazione finale del Manuale privacy, autorizzandone l'applicazione aziendale;
- è garante dell'implementazione dei principi di privacy by design e privacy by default nei processi di trattamento
- anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento e delle proprie istruzioni
- valuta i risultati della gestione relativa alla sicurezza dei dati personali, i rischi aziendali generali e di business connessi alla sicurezza dei dati personali, e di conseguenza prende le decisioni in merito agli interventi necessari;

- assicura la creazione, la conservazione, la disponibilità e l'aggiornamento delle planimetrie della struttura fisica e degli impianti aziendali.

Al fine di attuare le attività sopra descritte il Titolare del trattamento può avvalersi del supporto operativo di consulenti esterni esperti nel settore, conservando la responsabilità della conduzione del sistema.

5.3.2. Amministratore sistema informativo

HOSPITALIA SRL ha nominato un amministratore del sistema informativo individuato in …….

5.3.3. Responsabili del trattamento

Sono figure che operano all'interno di organizzazioni terze a cui l'organizzazione ha subappaltato uno o più processi che prevedono l'elaborazione di dati personali di cui è titolare HOSPITALIA SRL I contratti di riferimento specificano meglio le modalità e le tempistiche dei trattamenti. L'elenco è in Allegato 1

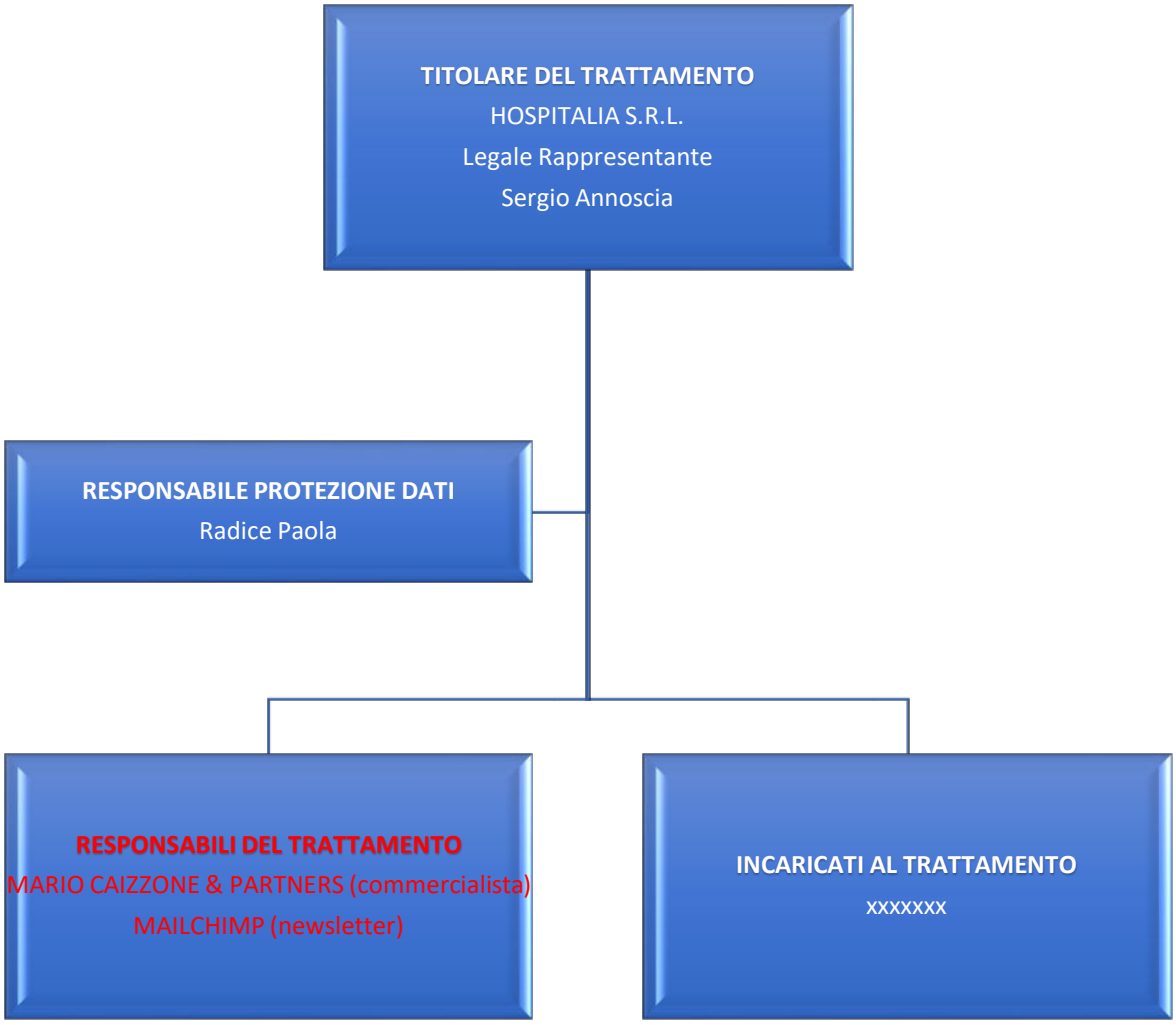
- definisce gli aspetti organizzativi (compiti e responsabilità) di dettaglio per la sicurezza dei dati personali;
- ha potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- assicura il riscontro all'interessato relativamente all'esercizio dei suoi diritti, in modo efficiente e senza ritardo;
- assicura la comunicazione dell'informativa ai soggetti interessati relativamente al trattamento dei dati personali che li riguardano;
- assicura la richiesta del consenso ai soggetti interessati nei casi previsti
- assicura, anche per mezzo di servizi esterni, la manutenzione ordinaria e programmata delle strutture e degli impianti, allo scopo di mantenerli in adeguato stato di efficienza e garantirne sia l'affidabilità sia la disponibilità;
- assicura la gestione delle emergenze relative alla sicurezza delle strutture fisiche e degli impianti che possono influire sulla sicurezza dei dati personali trattati dall'azienda;
- rileva gli elementi necessari per l'analisi e la valutazione dei rischi legati alla sicurezza dei dati personali nonché per l'individuazione delle idonee misure di sicurezza corrispondenti al tipo ed al livello dei rischi riscontrati nel corso di verifiche interne.

5.3.4. Incaricati dei trattamenti

Gli incaricati dei trattamenti (elenco in allegato 1):

- assicurano in modo preciso, responsabile e consapevole l'attuazione delle prescrizioni relative alla sicurezza dei dati personali contenute nel presente Manuale, attenendosi in modo specifico alle istruzioni impartite con l'attribuzione dell'incarico;
- segnalano con tempestività al Legale Rappresentante ogni rischio, problema, situazione di contesto o evento che si evidenzi negativo dal punto di vista della sicurezza dei dati personali.

ORGANIGRAMMA



6. TRATTAMENTI DI MASSIMA EFFETTUATI SUI DATI

L'incaricato preposto al trattamento dei dati personali deve operare seguendo le direttive del Legale rappresentante. L'incaricato deve organizzare il trattamento dei dati personali in sessioni. Ogni sessione consta di elementi peculiari che la identificano: trattamento, inizio, fine, avvertenze. L'elenco delle sessioni di trattamento è enumerato nella scheda seguente.

TRATTAMENTO	INIZIO	FINE	AVVERTENZE
La raccolta diretta	Compilazione di moduli di raccolta dati	Conservazione del supporto cartaceo in attesa di registrazione o elaborazione	Fornire l'informativa all'interessato Questo passaggio deve essere effettuato anche nel caso di primo contatto verbale dal vivo o telefonico
La raccolta indiretta	Ricezione di moduli o documenti contenente dati personali	Conservazione del supporto cartaceo	I dati sono raccolti in attesa di elaborazione. Conservazione analoga avviene per i preventivi contenenti dati personali
La registrazione	Trascrizione di dati personali in registri, elenchi, agende, rubriche, database ecc	Conservazione del supporto nel luogo di custodia	
La conservazione	Identificazione al fine di garantire la corretta conservazione	Conservazione nel luogo di custodia	
La consultazione	Ricerca ed estrazione di un documento al fine di acquisirne il contenuto	Archiviazione del documento nel luogo di custodia o passaggio ad altro trattamento	
L'elaborazione	Acquisizione dei dati di un documento al fine di produrre estratti, informazione, altri documenti	Archiviazione della produzione nel luogo di custodia	
La modifica	Consultazione di documenti al fine di aggiornare o incrementare o decrementare il contenuto	Conservazione dei faldoni nel luogo di custodia o passaggio ad altro trattamento	La modifica di un documento potrebbe produrre nuovi documenti in sostituzione di quelli meno aggiornati. in questo caso è necessario procedere alla distribuzione dei nuovi e marcare i precedenti come obsoleti documento prodotto
L'estrazione	Ricerca di dati da documenti, registri ed elenchi al fine di produrre nuovi documenti	Archiviazione o nel luogo di custodia o comunicazione dell'estratto	

TRATTAMENTO	INIZIO	FINE	AVVERTENZE
La diffusione	Sulla base di specifiche esigenze e progetti	Conservazione di una copia interna	Prevalentemente in forma anonima e avendo valutato attentamente le finalità
La limitazione	Su richiesta dell'interessato	Contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro	
La cancellazione	Consultazione di un documento al fine di annullarne il contenuto di dati personali	Trasformazione del documento in forma permanentemente anonima	
La distruzione	Consultazione di un documento al fine di distruggere fisicamente il supporto	Il supporto non consente più nessun trattamento dei dati personali	Nel processo di distruzione il dato personale non deve essere più leggibile

Per ogni sessione l'incaricato deve aver cura che i dati personali non siano accessibili a soggetti non autorizzati, siano sorvegliati, non siano utilizzati per finalità eccedenti ma solo in relazione alle funzioni aziendali e nel limite delle finalità per cui sono stati raccolti. L'incaricato deve rispettare le libertà fondamentali dell'interessato, non lederne la dignità, la riservatezza e deve essere ispirato da principi di correttezza, liceità, trasparenza. L'elenco degli incaricati al trattamento dei dati personali è redatto per classi omogenee.

7. REGISTRO TRATTAMENTI

7.1. Registro trattamenti del Titolare

Titolare del trattamento	**HOSPITALIA SRL** Via Marangon 10, 45010 Rosolina (RO) Codice fiscale e Partita IVA 09491140969
Responsabile Protezione Dati	Radice Paola Via Adamoli 12, 21100 Varese C.F. RDCPLA69S45E734R

Le attività di trattamento sono elencate nel seguito:

1. Gestione Personale
2. Gestione Contabilità
3. Gestione Ospiti
4. Gestione Videosorveglianza

DESCRIZIONE DEL TRATTAMENTO	
ID	1
Trattamento	Gestione dati del personale
Descrizione	È un processo standardizzato che prevede l'utilizzo dei dati minimi previsti dalle norme contrattuali e amministrative vigenti. È fornita un'informativa completa sui trattamenti, in particolare relativamente ai dati particolari. I dati sono trattati con rigorosa applicazione del principio di minimizzazione. Anche il flusso mensile di dati verso lo studio paghe che elabora gli stipendi è un processo standardizzato. Per quanto riguarda i documenti relativi alla medicina del lavoro, sono contenuti in buste sigillate a cui ha accesso solo il medico competente nominato dal Datore di Lavoro (Rif. D.Lgs.81/08 e smi) e sono conservate nell'ufficio della direzione non accessibile ad estranei c/o la struttura. La presente scheda include anche il trattamento dei dati del personale medico/infermieristico/OSS ecc fornito dalla cooperativa, per le specifiche finalità.
Data di creazione del trattamento	01/02/2020
Data di aggiornamento	-

Finalità del trattamento		Base giuridica del trattamento
Finalità principale	Gestione degli aspetti relativi al trattamento giuridico ed economico del personale e verifica del possesso dei requisiti per l'assunzione;	Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso, art. 6,1(b)
Altre finalità	Formazione professionale per il personale;	Obbligo legale per il titolare, art. 6,1(c);
Altre finalità	Adempimento di obblighi fiscali o contabili;	Obbligo legale per il titolare, art. 6,1(c);
Altre finalità	Igiene e sicurezza del lavoro.	Obbligo legale per il titolare, art. 6,1(c);
Altre finalità	Gestione degli aspetti derivanti dal Contratto per le prestazioni di servizi socio-sanitario-assistenziali forniti dal personale della cooperativa.	Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso, art. 6,1(b)

		Obbligo legale per il titolare, art. 6,1(c);

Categorie di dati personali comuni	Descrizione	Tempi di conservazione
Dati identificativi, stato civile; immagini ...	Nome; indirizzo; contatti (email/telefono); IBAN; Carta identità; codice fiscale; certificati vari (stato di famiglia, matrimonio, ecc); foto per tesserino riconoscimento.	Fine rapporto di lavoro. Per i dati contabili/fiscali vale la tempistica definita per legge ai fini contabili/fiscali.
Informazioni economiche e finanziarie (reddito, situazione finanziaria, situazione fiscale, ecc.)	Reddito	Fine rapporto di lavoro. Per i dati contabili/fiscali vale la tempistica definita per legge ai fini contabili/fiscali.
Dati inerenti situazioni giudiziarie civili, amministrative, tributarie;	-	Fine rapporto di lavoro. Per i dati contabili/fiscali vale la tempistica definita per legge ai fini contabili/fiscali.
Dati relativi alla famiglia e a situazioni personali.	Dati anagrafici figli, familiari a carico, certificati e dati richiesti dalle leggi applicabili (ad esempio legge 104)	Fine rapporto di lavoro. Per i dati contabili/fiscali vale la tempistica definita per legge ai fini contabili/fiscali.

Categorie di dati personali particolari	Descrizione	Tempi di conservazione
Stato di salute	Idoneità alla mansione	Fine rapporto di lavoro.

Destinatari	Tipo destinatari	Dettaglio
Destinatario 1	Incaricati interni al trattamento	Responsabile RSA
Destinatario 2	Responsabili del trattamento	Soggetti esterni incaricati di funzioni di manutenzione e

		assistenza dei sistemi informatici e di comunicazione, per sole finalità tecniche; Soggetti esterni consulenti in materia fiscale/contabile/consulente del lavoro, per sole finalità amministrative/fiscali RSPP/Medico competente
Destinatario 3	Enti vari	Enti Pubblici (Inps, Inail, Direzione Provinciale del Lavoro, Uffici fiscali ecc.), Fondi o casse private di previdenza e assistenza, studi medici in adempimento degli obblighi in materia di igiene e sicurezza sul lavoro, società di assicurazioni, istituti di credito, organizzazioni sindacali cui lei abbia conferito specifico mandato, Fondi integrativi, Organizzazioni imprenditoriali cui aderisce l'azienda, Organismi di Vigilanza, Autorità Giudiziarie nonché a tutti gli altri soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle finalità suddette

Misure di sicurezza	Tipologia	Dettaglio
Misure di sicurezza 1	Misure organizzative	Minimizzazione della quantità di dati personali; Gestione dei Responsabili del trattamento e

		delle terze parti; Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali; Gestione e formazione del personale; Controllo degli accessi fisici; Videosorveglianza; Sicurezza dei documenti cartacei.
Misure di sicurezza 2	**Misure tecniche**	Autenticazione degli utenti; **Gestione delle autorizzazioni; Gestione sicura delle postazioni di lavoro; Cifratura e pseudonimizzazione; Protezione delle fonti di rischio ambientali; Gestione backup.**

Trasferimento extra UE	Destinatario	Paese	Tipo di garanzia	Link alla documentazione
Destinatario 1	**Nessun trasferimento extra EU**			

DESCRIZIONE DEL TRATTAMENTO	
ID	2
Trattamento	Gestione dati contabilità
Descrizione	È il processo standardizzato di gestione della contabilità aziendale, sulla base delle norme contabili e fiscali applicabili. Le attività sono gestite sia con modalità cartacea che elettronica dall'ufficio amministrazione e i documenti sono trasmessi periodicamente al commercialista.
Data di creazione del trattamento	01/02/2020
Data di aggiornamento	-

Finalità del trattamento		Base giuridica del trattamento
Finalità principale	Adempimento di obblighi fiscali o contabili.	Obbligo legale per il titolare, art. 6,1(c);
Altre finalità	Gestione clienti	Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso, art. 6,1(b)
Altre finalità	Gestione fornitori	Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso, art. 6,1(b)

Categorie di dati personali comuni	Descrizione	Tempi di conservazione
Dati identificativi, stato civile; immagini ...	Ragione sociale; indirizzo; contatti (email/telefono); partita IVA; IBAN	Per i dati contabili/fiscali vale la tempistica definita per legge ai fini contabili/fiscali.

Categorie di dati personali particolari	Descrizione	Tempi di conservazione
Stato di salute	N/A	

Destinatari	Tipo destinatari	Dettaglio
Destinatario 1	Incaricati interni al trattamento	Responsabile RSA
Destinatario 2	Responsabili del trattamento	Soggetti esterni incaricati di funzioni di manutenzione e assistenza dei sistemi informatici e di comunicazione, per sole finalità tecniche; Soggetti esterni consulenti in materia fiscale/contabile, per sole finalità amministrative/fiscali
Destinatario 3	Enti vari	Enti Pubblici (Agenzia delle Entrate, ecc.), Banche

Misure di sicurezza	Tipologia	Dettaglio
Misure di sicurezza 1	Misure organizzative	Minimizzazione della quantità di dati personali; Gestione dei Responsabili del trattamento e delle terze parti; Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali; Gestione e formazione del personale; Controllo degli accessi fisici; Videosorveglianza; Sicurezza dei documenti cartacei.
Misure di sicurezza 2	Misure tecniche	Autenticazione degli utenti; Gestione delle autorizzazioni; Gestione sicura delle postazioni di lavoro; Cifratura e pseudonimizzazione; Protezione delle fonti di rischio ambientali; Gestione backup.

Trasferimento extra UE	Destinatario	Paese	Tipo di garanzia	Link alla documentazione
Destinatario 1	Nessun trasferimento extra EU			

DESCRIZIONE DEL TRATTAMENTO	
ID	3
Trattamento	Gestione dati ospiti
Descrizione	Essendo la RSA una struttura convenzionata, la Regione Veneto fornisce il software gestionale per la gestione sia dei dati degli ospiti, che per il flusso sia economico che di presenze.
Data di creazione del trattamento	01/02/2020
Data di aggiornamento	-

Finalità del trattamento		Base giuridica del trattamento
Finalità principale	• attività di prevenzione, diagnosi, cura, riabilitazione, assistenza, anche alberghiera, ovvero al complesso di prestazioni svolte dalla Casa di Riposo a tutela della Sua salute e/o incolumità fisica; • gestione di casi di emergenza sanitaria; • utilizzo di tutti i servizi complementari richiesti, che fanno parte del contratto e dell'incarico che ci viene affidato in relazione della sua presenza quale ospite della Casa di Riposo; • esame della domanda di ammissione al fine di utilizzare da parte Sua in tutto od in parte i servizi della Casa di Riposo;	Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso, art. 6,1(b) I dati sullo stato di salute sono trattati ai sensi dell'art. 9, comma 2 punto h) del GDPR e, in accordo all'art. 9 comma 3 del GDPR, da o sotto la responsabilità di un professionista soggetto al segreto professionale.
Altre finalità	• adempimento di ogni obbligo a carico del Titolare del trattamento che sia previsto da leggi, regolamenti e	Obbligo legale per il titolare, art. 6,1(c);

	normative sia in ambito fiscale, sanitario, ecc. in relazione alla Sua presenza quale ospite della Casa di Riposo; • svolgimento di attività amministrative, fiscali o contabili interne connesse al rapporto cliente-fornitore e per adempiere agli obblighi in genere previsti a carico del Titolare del trattamento da leggi o da regolamenti, dalla normativa comunitaria, da richieste dell'Autorità giudiziaria oppure per esercitare i diritti del Titolare (ad esempio il diritto di difesa in giudizio).	

Categorie di dati personali comuni	Descrizione	Tempi di conservazione
Dati identificativi, stato civile; immagini ...	Dati anagrafici; Codice fiscale ed altri numeri di identificazione personale; Carte sanitarie; Dati riguardanti i suoi familiari/componenti del nucleo familiare/curatori o a situazioni personali; Identificativo IBAN del conto corrente bancario.	I dati personali e particolari verranno conservati per il tempo previsto dall'attuale normativa: in particolare, i dati relativi a ciascun episodio assistenziale, raccolti nella relativa scheda sanitaria, verranno conservati a tempo indeterminato, perdurando il rapporto contrattuale di cura. Al termine del rapporto contrattuale di cura, conserverà i dati per un periodo non superiore al termine prescrizionale di legge per la tutela dei propri diritti legali e di difesa.

Categorie di dati personali particolari	Descrizione	Tempi di conservazione
Stato di salute	Stato di salute; Patologie attuali e pregresse; Terapie in corso;	I dati personali e particolari verranno conservati per il tempo previsto dall'attuale normativa: in particolare, i dati relativi a ciascun episodio assistenziale, raccolti nella relativa scheda sanitaria, verranno conservati a tempo indeterminato, perdurando il rapporto contrattuale di cura. Al termine del rapporto contrattuale di cura, conserverà i dati per un periodo non superiore al
Convinzioni religiose	Convinzioni religiose;	

		termine prescrizionale di legge per la tutela dei propri diritti legali e di difesa.

Destinatari	Tipo destinatari	Dettaglio
Destinatario 1	Incaricati interni al trattamento	Responsabile RSA; Soggetti interni alla Casa di Riposo con funzione di Incaricati al trattamento; Professionisti medici e personale sanitario, anche con rapporto di collaborazione occasionale con la Casa di Riposo; Enti, società, gruppi o persone fisiche, anche volontarie, che si occupano dell'assistenza degli ospiti sia in ambito sanitario che in ogni altro ambito facente parte delle prestazioni che la Casa di Riposo offre ai propri ospiti; Azienda Ulss competente per la Regione Veneto;
Destinatario 2	Responsabili del trattamento	Cooperativa per le prestazioni di servizi socio-sanitario-assistenziali Soggetti esterni incaricati di funzioni di manutenzione e assistenza dei sistemi informatici e di comunicazione, per sole finalità tecniche; Soggetti esterni consulenti in materia fiscale/contabile, per sole finalità amministrative/fiscali
Destinatario 3	Enti vari	Autorità ed Enti Pubblici competenti per obbligo di legge

Misure di sicurezza	Tipologia	Dettaglio
Misure di sicurezza 1	Misure organizzative	Minimizzazione della quantità di dati personali; Gestione dei Responsabili del trattamento e delle terze parti; Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali; Gestione e

		formazione del personale; Controllo degli accessi fisici; Videosorveglianza; Sicurezza dei documenti cartacei.
Misure di sicurezza 2	Misure tecniche	Autenticazione degli utenti; Gestione delle autorizzazioni; Gestione sicura delle postazioni di lavoro; Cifratura e pseudonimizzazione; Protezione delle fonti di rischio ambientali; Gestione backup.

Trasferimento extra UE	Destinatario	Paese	Tipo di garanzia	Link alla documentazione
Destinatario 1	Nessun trasferimento extra EU			

DESCRIZIONE DEL TRATTAMENTO	
ID	4
Trattamento	Gestione dati videosorveglianza
Descrizione	Il sistema videosorveglianza riprende aree esterne e interne (aree comuni). Nel rispetto della normativa vigente, appositi cartelli informano gli interessati che stanno per accedere o che si trovano nella zona videosorvegliata. È disponibile autorizzazione dell'Ispettorato del Lavoro.
Data di creazione del trattamento	01/02/2020
Data di aggiornamento	-

Finalità del trattamento		Base giuridica del trattamento
Finalità principale	• Tutela dell'incolumità fisica degli ospiti, tramite la prevenzione di situazioni potenzialmente pericolose • Sorveglianza contro intrusioni da parte di terzi • Tutela della sicurezza dei lavoratori; • Tutela del patrimonio aziendale.	Il trattamento dei dati si fonda sul legittimo interesse. Il rifiuto di conferire i dati comporta l'impossibilità di consentire all'interessato l'accesso alle sedi del Titolare. L'accesso alle zone videosorvegliate comporta la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo delle immagini degli interessati.

Categorie di dati personali comuni	Descrizione	Tempi di conservazione
Dati identificativi, stato civile; immagini ...	Immagini	Le immagini registrate saranno cancellate nei termini previsti dal Garante (dopo 24 ore, salvo festivi o altri casi di chiusura dell'esercizio, e comunque non oltre una settimana) e non saranno oggetto di comunicazione a terzi, tranne nel caso in cui si debba aderire ad una specifica

		richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria).

Categorie di dati personali particolari	Descrizione	Tempi di conservazione
	N/A	

Destinatari	Tipo destinatari	Dettaglio
Destinatario 1	Incaricati interni	Responsabile RSA
Destinatario 2	Responsabili del trattamento	Soggetti esterni incaricati di funzioni di manutenzione e assistenza dei sistemi informatici e di comunicazione, per sole finalità tecniche;
Destinatario 3	Enti vari	Autorità giudiziaria o di polizia giudiziaria

Misure di sicurezza	Tipologia	Dettaglio
Misure di sicurezza 1	Misure organizzative	Minimizzazione della quantità di dati personali; Gestione dei Responsabili del trattamento e delle terze parti; Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali; Gestione e formazione del personale; Controllo degli accessi fisici; Videosorveglianza; Sicurezza dei documenti cartacei.
Misure di sicurezza 2	Misure tecniche	Autenticazione degli utenti; Gestione delle autorizzazioni; Gestione sicura delle postazioni di lavoro; Cifratura e pseudonimizzazione; Protezione delle fonti di rischio ambientali; Gestione backup.

Trasferimento extra UE	Destinatario	Paese	Tipo di garanzia	Link alla documentazione
Destinatario 1	Nessun trasferimento extra EU			

8. SISTEMI INFORMATIVI E PROTEZIONE DI AREE E LOCALI

HOSPITALIA SRL ha affidato la manutenzione della rete informatica della RSA di Rosolina a Cyberia Informatica snc, Via Roma 57, 25015 Desenzano del Garda (BS), P.iva e Cod Fisc: 02795270988, nominata Responsabile del Trattamento.

8.1. Autenticazione informatica e procedure di gestione delle credenziali di autenticazione

Il trattamento di dati personali con strumento elettronico è subordinato al superamento di una procedura di identificazione elettronica.

Gli strumenti elettronici che compongono il sistema informatico aziendale, e che trattano o ospitano dati personali, sono stati predisposti per non consentire accessi ad utenti anonimi. Ogni strumento elettronico richiederà all'inizio delle sessioni di lavoro un nome utente ed una password. Questa coppia di informazioni costituiscono le credenziali di autenticazione.

Gli incaricati che ricevono in custodia le credenziali di autenticazione devono custodirle adottando le opportune cautele:

- Scegliere una password facile da ricordare in modo da non avere la necessità di trascriverla;
- In sede di utilizzo si deve proteggere la digitazione da occhi indiscreti;

La formazione e la scelta della password deve tenere conto dei seguenti accorgimenti:

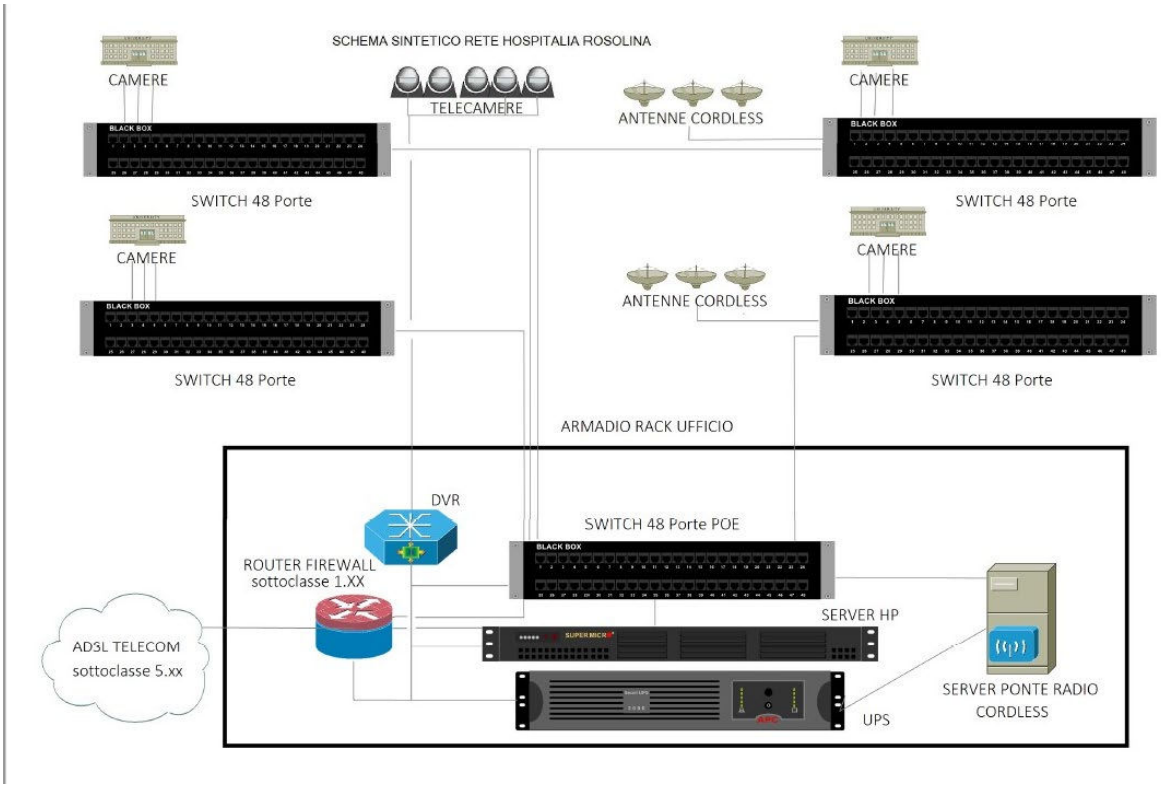
- Al primo utilizzo delle credenziali l'incaricato dovrà modificare la password garantendo il requisito di segretezza;
- La password dovrà essere modificata ogni sei mesi o ogni tre mesi se nell'unità organizzativa sono trattati anche dati particolari. In relazione all'unità organizzativa di appartenenza ogni incaricato dovrà cambiare la propria password seguendo lo schema qui illustrato;
- La password deve essere composta da almeno otto caratteri: è opportuno che contenga una combinazione di caratteri maiuscoli e minuscoli e di numeri;
- La scelta della password non deve avere riferimenti diretti all'incaricato, al nome utente, all'unità organizzativa in modo da non renderla facilmente identificabile.
- Il nome utente una volta utilizzato non è più scindibile dall'incaricato a cui è stato assegnato: se un incaricato viene destinato ad altre mansioni il suo nome utente, non più in uso, non potrà essere riassegnato a nuovi operatori. L'incaricato che riprende le sue funzioni dopo un periodo di sospensione, nel corso del quale le sue credenziali sono state disabilitate, potrà richiedere il ripristino del suo nome utente.

Le credenziali sono disattivate d'ufficio o su richiesta dell'incaricato nel caso in cui vi sia il timore o la certezza che la password sia stata violata o non rispetta i requisiti sostanziali; In questo caso le credenziali di autenticazione disattivate non sono più ripristinabili ed all'incaricato verranno riassegnate delle nuove credenziali di autenticazione.

8.2. Configurazione rete

Ogni utente dispone di un proprio account aziendale, che attraverso login e password, può accedere alla cartella condivisa sulla rete aziendale. Tali credenziali rappresentano la carta d'identità all'interno della rete, registrando ogni attività svolta nell'Active Directory.

Di seguito si riporta schema della rete HOSPITALIA ROSOLINA.



8.3. La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da:

- dispositivi antincendio (estintori);
- videosorveglianza.

9. CONSERVAZIONE E TRATTAMENTI SUI DATI CARTACEI

9.1. Generalità sulla gestione del dato cartaceo

La struttura è presidiata negli orari di apertura. L'accesso alla struttura è possibile solo previo riconoscimento del visitatore (fornitori, utenti, consulenti, ecc.).

Inoltre:

- Adotta buone pratiche di gestione della documentazione che garantiscono la corretta conservazione, reperibilità, accesso alla documentazione.
- Ha definito l'ubicazione, la responsabilità, il tempo di conservazione e le misure di protezione della documentazione sensibile ai fini del trattamento dei dati personali
- Ha sensibilizzato i propri incaricati sui rischi connessi con i trattamenti cartacei e con il lasciare incustodita la documentazione cartacea durante il trattamento. Gli incaricati sono formati e implementano le misure di prevenzione e protezione definite.
- Per quanto riguarda i fornitori esterni di prodotti e servizi che per ragioni tecniche accedono ai locali aziendali, il responsabile aziendale che riceve il fornitore deve assicurare il presidio delle operazioni fino al termine dell'intervento ed all'uscita dall'azienda, se non diversamente stabilito nell'ambito del contratto in essere
- Tutto il personale inoltre deve:
  - assicurare la cura nella gestione delle informazioni e dei documenti utilizzati, ricevuti, in attesa di smistamento o trasmissione, in modo da non renderli visibili e comunque consultabili da persone esterne in visita; assicurare in ogni caso la riservatezza delle informazioni trattate in modo scritto (appunti, ecc.), verbalmente o telefonicamente rispetto a persone presenti che potrebbero vederle o ascoltarle;
  - non fornire a persone esterne (presenti o per telefono) informazioni riservate relative all'azienda o al personale interno;
  - segnalare tempestivamente al Titolare eventuali emergenze relative alla violazione ed alla sicurezza degli accessi all'Azienda.

TABELLA RIASSUNTIVA UBICAZIONE DATI CARTACEI

Tipo DatI	**Ubicazione**	**Responsabile**	**Protezione**	**Tempo conservazione**
Contabilità	Sede Titolare Trattamento	Responsabile del Trattamento	Ufficio non accessibile ad estranei o persone non autorizzate. Videosorveglianza. Estintori.	Norme di legge contabile/fiscale
Personale	Sede Titolare Trattamento	Responsabile del Trattamento	Ufficio non accessibile ad estranei o persone non autorizzate. Videosorveglianza. Estintori.	Cessazione rapporto di lavoro e norme di legge contabile e fiscale
Ospiti	Sede Titolare Trattamento	N/A	Ufficio non accessibile ad estranei o persone non autorizzate. Videosorveglianza. Estintori.	Il Titolare tratterà i dati personali per il tempo della permanenza dell'ospite e successivamente secondo norme di legge applicabile.

9. ANALISI E VALUTAZIONE DEL RISCHIO

9.1. Analisi e valutazione del rischio

L'analisi e valutazione del rischio viene svolta attraverso le seguenti fasi:

1. Identificazione del rischio
2. Analisi del rischio
3. Ponderazione del rischio
4. Trattamento del rischio
5. Valutazione di impatto

L'analisi e valutazione del rischio, così come la valutazione d'impatto, rappresenta un "processo continuo" da riesaminare periodicamente ovvero ogniqualvolta vi sia un mutamento significativo circa la natura, la finalità o le modalità del trattamento, ivi compresa l'introduzione di nuove tecnologie. Le attività di riesame e aggiornamento sono dunque momenti rilevanti nel processo di valutazione d'impatto, poiché sono volti ad evitare che eventuali mutamenti incidano sull'osservanza della disciplina, garantendo così la costante conformità al Regolamento.

9.1.1. Identificazione del rischio

In seguito all'analisi dei flussi di processo dei dati e relativi trattamenti, sono stati individuati i rischi.

9.1.2. Analisi del rischio

A ciascun elemento di valutazione (probabilità/gravità/fattori) è stato assegnato un coefficiente nel rispetto della tabella che segue:

PROBABILITA'		*GRAVITA'*	
1	Improbabile: non appare possibile che le fonti di rischio possano creare una minaccia.	1	Lieve: inconvenienti superabili senza difficoltà.
2	Poco probabile: appare difficile che le fonti di rischio possano creare una minaccia.	2	Medio: inconvenienti significativi, superabili nonostante alcune difficoltà.
3	Probabile: appare possibile che le fonti di rischio possano creare una minaccia.	4	Grave: conseguenze significative, superabili solo con difficoltà.
4	Molto probabile: appare estremamente facile che le fonti di rischio possano creare una minaccia.	16	Molto grave: conseguenze significative, anche irrimediabili, che potrebbero non superare.

9.1.3. Ponderazione del rischio

La valutazione del rischio specifico che riaccada tale fenomeno, ottenuta tramite la valutazione congiunta della probabilità/impatto/fattori d'influenza, viene compiuta secondo la tabella che segue:

IMPATTO / PROBABILITA'		Lieve	Medio	Grave	Molto grave
		1	**2**	**4**	**8**
Improbabile	**1**	1	2	4	8
Poco probabile	**2**	2	4	8	16
Probabile	**3**	3	6	12	24
Molto probabile	**4**	4	8	16	32

A seguito del processo suesposto la ponderazione del rischio è stata effettuata nel rispetto della seguente tabella:

Ponderazione del rischio:

Esito (punteggio)	Conseguenza:
1 a 3	RISCHIO ACCETTABILE per la corretta gestione del sistema
4 a 6	RISCHIO BASSO per la corretta gestione del sistema
8 a 12	RISCHIO MEDIO per la corretta gestione del sistema
> 12	RISCHIO ELEVATO per la corretta gestione del sistema

9.1.4. Trattamento del rischio

Per ogni rischio poi sono state valutate le misure di prevenzione e protezione.

VALUTAZIONE DEI RISCHI						
ID	**Trattamento**	**Rischio**		**MPP**	**Stima rischio residuo**	**Accettabilità**
1	ORGANIZZAZIONE	Sono effettuati trattamenti che possono presentare un rischio per i diritti e le libertà degli interessati?	SI	La struttura tratta una quantità di dati che non può essere definita su "larga scala" (n. 120 posti letto autorizzati di cui 96 posti letto accreditati dalla Regione Veneto per anziani non autosufficienti totali o parziali). Sono applicate adeguate misure di sicurezza sia organizzative che tecnologiche.	Rischio BASSO [P1]X[D4]=4	SI
1a	ORGANIZZAZIONE	E' stata valutata la necessità di eseguire la valutazione di impatto?	SI	La struttura, non esegue un trattamento dati su larga scala, quindi non si ritiene per il momento necessario eseguire la valutazione di impatto.	Rischio BASSO [P1]X[D4]=4	SI
2	ORGANIZZAZIONE	Il trattamento include "categorie particolari di dati di cui all'articolo 9, paragrafo 1 (che sono gli odierni dati particolari, con l'aggiunta dei dati genetici e biometrici), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10"?	SI	Dati sullo stato di salute e delle convinzioni religiose.	Rischio BASSO [P1]X[D4]=4	SI
3	ORGANIZZAZIONE	Il registro dei trattamenti è predisposto e aggiornato?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
4	ORGANIZZAZIONE	Sono indicati il nome e i dati di contratto, ove sussistenti: - del contitolare del trattamento? - del rappresentante del titolare del trattamento? - del responsabile della protezione dei dati?	SI	Nomina RPD e Capitolo 7 Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
5	ORGANIZZAZIONE	Sono esplicitate le finalità dei trattamenti effettuati?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
6	ORGANIZZAZIONE	Per ciascun trattamento sono individuate le categorie di interessati (ad es., dipendenti, clienti/utenti, fornitori, ecc.)?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
7	ORGANIZZAZIONE	Per ciascun trattamento sono individuate le categorie di dati, sono cioè rintracciati: - dati che rivelano l'origine razziale o etnica? - dati che rivelano le opinioni politiche? - dati che rivelano le convinzioni religiose o filosofiche? - dati che rivelano l'appartenenza sindacale? - dati genetici? - dati biometrici? - dati relativi alla salute? - dati relativi alla vita/orientamento sessuale? - dati relativi a condanne penali e reati?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
8	ORGANIZZAZIONE	Per ciascun trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
9	ORGANIZZAZIONE	Vi sono trattamenti in cui i dati sono comunicati a destinatari di Paesi terzi ovvero di organizzazioni internazionali?	NO			
10	ORGANIZZAZIONE	Contiene il registro l'indicazione dei trattamenti che includono i trasferimenti di	N/A			

ID	Trattamento	Rischio		MPP	Stima rischio residuo	Accettabilità
		dati personali verso un paese Terzo o un'organizzazione internazionale?				
11	ORGANIZZAZIONE	Il registro include l'identificazione del paese terzo o dell'organizzazione internazionale?	N/A			
12	ORGANIZZAZIONE	E' individuata la base giuridica (ad es., contratto, legge, standard internazionale, ecc.) di ciascun trattamento?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
13	ORGANIZZAZIONE	Sono indicati i termini ultimi previsti per la cancellazione delle diverse categorie di dati?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
14	ORGANIZZAZIONE	Sono descritte le misure di sicurezza tecniche e quelle organizzative a titolo di esempio: - la pseudonimizzazione e la cifratura dei dati personali? - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico? - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?	SI	Capitolo 7 del Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
15	ORGANIZZAZIONE	Dette misure garantiscono un livello di sicurezza adeguato al rischio?	SI		Rischio BASSO [P1]X[D4]=4	SI
16	ORGANIZZAZIONE	E' pianificato il riesame dell'adeguatezza delle misure di sicurezza?	SI	E' stabilito un riesame con frequenza annuale, oltre ad audit periodici di controllo svolti da RPD	Rischio BASSO [P1]X[D4]=4	SI
17	ORGANIZZAZIONE	Sono individuati e nominati i responsabili del trattamento?	SI	Allegato 1.1 Manuale Privacy	Rischio BASSO [P1]X[D4]=4	SI
18	ORGANIZZAZIONE	Gli incaricati al trattamento sono adeguatamente formati?	SI	E' stata consegnata una dispensa informativa	Rischio BASSO [P1]X[D4]=4	SI
19	GESTIONE DATI PERSONALE	Dipendente non è informato sui trattamenti che lo riguardano/non ha chiari i suoi diritti	NO	Informativa chiara	Rischio ACCETTABILE [P1]X[D2]=2	SI
20	GESTIONE DATI PERSONALE	Dati dipendente sono oggetto di trattamenti accessori per cui non ha rilasciato il consenso	NO	Attenzione alla richiesta degli opportuni consensi per trattamenti accessori	Rischio ACCETTABILE [P1]X[D2]=2	SI
21	GESTIONE DATI PERSONALE	Incaricato non è preparato sulle modalità di trattamento dei dati	NO	Incaricati adeguatamente formati / informati Incaricati con provata esperienza	Rischio ACCETTABILE [P1]X[D2]=2	SI
21A	GESTIONE DATI PERSONALE	Outsourcer non ha consapevolezza dei suoi obblighi e responsabilità rispetto alla privacy	NO	Nomina responsabile esterno	Rischio ACCETTABILE [P1]X[D2]=2	SI
21B	GESTIONE DATI PERSONALE	Outsourcer non ha adottato misure di sicurezza adeguate	NO	Attenta selezione del fornitore. Nomina responsabile esterno	Rischio ACCETTABILE [P1]X[D2]=2	SI
22	GESTIONE DATI CONTABILITA'	Cliente / Fornitore non è informato sui trattamenti che lo riguardano/non ha chiari i suoi diritti	NO	Informativa chiara	Rischio ACCETTABILE [P1]X[D2]=2	SI
23	GESTIONE DATI CONTABILITA'	Dati Cliente /Fornitore sono oggetto di trattamenti accessori per cui non ha rilasciato il consenso	NO	Attenzione alla richiesta degli opportuni consensi per trattamenti accessori	Rischio ACCETTABILE [P1]X[D2]=2	SI

ID	Trattamento	Rischio		MPP	Stima rischio residuo	Accettabilità
24	GESTIONE DATI CONTABILITA'	Incaricato non è preparato sulle modalità di trattamento dei dati	NO	Incaricati adeguatamente formati / informati Incaricati con provata esperienza	Rischio ACCETTABILE [P1]X[D2]=2	SI
24A	GESTIONE DATI CONTABILITA'	Outsourcer non ha consapevolezza dei suoi obblighi e responsabilità rispetto alla privacy	NO	Nomina responsabile esterno	Rischio ACCETTABILE [P1]X[D2]=2	SI
24B	GESTIONE DATI CONTABILITA'	Outsourcer non ha adottato misure di sicurezza adeguate	NO	Attenta selezione del fornitore. Nomina responsabile esterno	Rischio ACCETTABILE [P1]X[D2]=2	SI
25	GESTIONE OSPITI	Assistito non è informato sui trattamenti che lo riguardano/non ha chiari i suoi diritti	NO	Informativa chiara	Rischio BASSO [P1]X[D4]=4	SI
26	GESTIONE OSPITI	Dati Assistito sono oggetto di trattamenti accessori per cui non ha rilasciato il consenso	NO	Attenzione alla richiesta degli opportuni consensi per trattamenti accessori	Rischio BASSO [P1]X[D4]=4	SI
27	GESTIONE OSPITI	Incaricato non è preparato sulle modalità di trattamento dei dati	NO	Incaricati adeguatamente formati / informati Incaricati con provata esperienza	Rischio BASSO [P1]X[D4]=4	SI
27A	GESTIONE OSPITI	Outsourcer non ha consapevolezza dei suoi obblighi e responsabilità rispetto alla privacy	NO	Nomina responsabile esterno	Rischio BASSO [P1]X[D4]=4	SI
27B	GESTIONE OSPITI	Outsourcer non ha adottato misure di sicurezza adeguate	NO	Attenta selezione del fornitore. Nomina responsabile esterno	Rischio BASSO [P1]X[D4]=4	SI
28	GESTIONE DATI CARTACEI	Accesso illegittimo ai dati da parte di persone esterne o interne non autorizzate	-	I dati personali sono conservati in un locale non accessibile al pubblico. Al fine di prevenire l'ingresso da parte di persone non autorizzate ai locali in cui sono custoditi i dati personali l'accesso a terzi durante l'orario di lavoro è possibile solo in presenza del personale interno.	Rischio ACCETTABILE [P1]X[D2]=2	SI
29	GESTIONE DATI CARTACEI	Furto o sottrazione del documento cartaceo	-	Accessi sorvegliati.	Rischio ACCETTABILE [P1]X[D2]=2	SI
30	GESTIONE DATI CARTACEI	"Condivisione" involontaria dei dati cartacei durante le sessioni di trattamento	-	Lettera di incarico al trattamento dei dati personali. Formazione adeguata	Rischio ACCETTABILE [P1]X[D2]=2	SI
31	GESTIONE DATI CARTACEI	Errori nell'archiviazione dei dati	-	Buone prassi gestione della documentazione	Rischio ACCETTABILE [P1]X[D2]=2	SI
32	GESTIONE DATI CARTACEI	Errori nella tempistica di conservazione	-	Buone prassi gestione della documentazione	Rischio ACCETTABILE [P1]X[D2]=2	SI
33	GESTIONE DATI CARTACEI	Possibilità di incendio nei locali	-	I locali sono dotati di appositi estintori da utilizzarsi per l'estinzione delle fiamme in caso di incendio.	Rischio BASSO [P1]X[D4]=4	SI
34	GESTIONE DATI CARTACEI	Incapacità di gestire il data breach	-	Misure di sicurezza che minimizzino la probabilità e l'impatto del Data breach Definita procedura gestione del data breach Nominato RPD	Rischio ACCETTABILE [P1]X[D2]=2	SI
35	GESTIONE SISTEMI INFORMATICI	Accesso illegittimo ai dati da parte di persone esterne all'organizzazione o interne non autorizzate	-	L'accesso a terzi ai locali durante l'orario di lavoro è possibile solo in presenza del personale interno.	Rischio ACCETTABILE [P1]X[D2]=2	SI
36	GESTIONE SISTEMI INFORMATICI	Rischi connessi con perdita, furto e uso improprio di credenziali di accesso ai portali e token	-	Credenziali personali.	Rischio ACCETTABILE [P1]X[D2]=2	SI
37	GESTIONE SISTEMI INFORMATICI	Modifiche non autorizzate ai dati	-	Credenziali personali	Rischio ACCETTABILE [P1]X[D2]=2	SI

ID	Trattamento	Rischio		MPP	Stima rischio residuo	Accettabilità
38	GESTIONE SISTEMI INFORMATICI	Possibilità di eventuali furti dai locali di uno o più strumenti contenenti i dati oggetto del trattamento o smarrimento degli stessi	-	L'accesso a terzi ai locali durante l'orario di lavoro è possibile solo in presenza del personale interno.	Rischio ACCETTABILE [P1]X[D2]=2	SI
39	GESTIONE SISTEMI INFORMATICI	Possibilità di guasto all'impianto elettrico che causi gravi danni e/o cortocircuiti alle attrezzature elettroniche contenenti i dati oggetto di trattamento	-	L'impianto elettrico è certificato ai sensi di Legge. Inoltre le apparecchiature elettroniche contenenti i dati oggetto del trattamento sono collegate alla rete elettrica tramite apposite prese antifulmine e protette contro gli sbalzi di tensione.	Rischio ACCETTABILE [P1]X[D2]=2	SI
40	GESTIONE SISTEMI INFORMATICI	Possibilità di allagamento dei locali	-	L'eventuale allagamento (improbabile) potrebbe derivare da guasti sugli impianti. Per evitare il più possibile eventuali danneggiamenti alle apparecchiature elettroniche contenenti i dati oggetto del trattamento a causa di eventuale allagamento dei locali, esse sono poste in posizione rialzata da terra.	Rischio ACCETTABILE [P1]X[D2]=2	SI
41	GESTIONE SISTEMI INFORMATICI	Possibilità di incendio nei locali	-	I locali sono dotati di appositi estintori da utilizzarsi per l'estinzione delle fiamme in caso di incendio.	Rischio BASSO [P1]X[D4]=4	SI
42	GESTIONE SISTEMI INFORMATICI	Possibilità di utilizzo degli strumenti da parte di persone non autorizzate	-	Controllo degli accessi logici ed autenticazione	Rischio ACCETTABILE [P1]X[D2]=2	SI
43	GESTIONE SISTEMI INFORMATICI	Possibilità di causare guasti alla strumentazione hardware o software dovuti a mancanza di formazione, scarsa attenzione o incuria da parte del personale.	-	Personale informato sul corretto uso degli strumenti informatici.	Rischio ACCETTABILE [P1]X[D2]=2	SI
44	GESTIONE SISTEMI INFORMATICI	Possibilità di infezione da virus informatici, spyware o malware	-	Antivirus	Rischio BASSO [P1]X[D4]=4	SI
45	GESTIONE SISTEMI INFORMATICI	Possibilità di eventuali guasti alla strumentazione elettronica utilizzata per il trattamento dei dati.	-	Cura nel rinnovare hardware.	Rischio BASSO [P1]X[D4]=4	SI
46	GESTIONE SISTEMI INFORMATICI	Possibilità che le copie di backup della banca dati non siano più riutilizzabili a causa di degrado dei supporti di memorizzazione utilizzati.	-	Sostituzione periodica dei dispositivi	Rischio BASSO [P1]X[D4]=4	SI
47	GESTIONE SISTEMI INFORMATICI	Incapacità di gestire il data breach	-	Misure di sicurezza che minimizzino la probabilità e l'impatto del Data breach Definita procedura gestione del data breach Nominato RDP	Rischio ACCETTABILE [P1]X[D2]=2	SI

9.2. Programma di miglioramento

ID	Trattamento	Rischio		MPP	Rischio residuo atteso	Responsabile	Accettabilità

Nessuna azione individuata.

9.3. Valutazione di impatto

La prima fase del processo di valutazione d'impatto concerne l'esame dell'obbligatorietà di condurre la valutazione d'impatto. Il Regolamento offre un elenco di tre ipotesi di trattamento in cui la valutazione è obbligatoria, ma lascia alle autorità di controllo (leggasi: i Garanti di ciascun Stato membro) il compito di redigere un elenco delle tipologie di trattamenti soggetti al requisito. Ai sensi dell'art. 35, 3° comma del Regolamento, la valutazione d'impatto è obbligatoria in presenza di:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato;

b) un trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;

c) una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Una volta stabilito se procedere alla valutazione d'impatto rappresenta una scelta obbligatoria o facoltativa, occorrerà effettuare una ricognizione sistematica dei trattamenti che presentino un rischio elevato.

Ove sulla base della valutazione d'impatto il titolare del trattamento sia riuscito a porre rimedio in modo soddisfacente ai rischi emersi, la procedura può dirsi conclusa. In caso contrario, cioè qualora la situazione di rischio non sia stata mitigata e il trattamento riveli pertanto un rischio ancora elevato per i diritti e le libertà fondamentali dei soggetti interessati, occorrerà rivolgersi all'autorità di controllo (nel caso di specie, l'Autorità Garante italiana per la protezione dei dati personali) al fine di avviare la c.d. consultazione preventiva ai sensi dell'art. 36 del Regolamento.

HOSPITALIA SRL

- per la tipologia di dati trattati e dei rischi rilevati,
- viste le indicazioni del Garante Privacy del 15/11/2018 (doc.web n. 9058979) pubblicate sulla Gazzetta Ufficiale serie generale n. 269 del 19/11/2018,

La struttura di Rosolina di HOSPITALIA SRL pur trattando dati relativi a categorie particolari di dati personali particolari, quali dati sullo stato di salute degli ospiti della struttura, in termini numerici non è associabile ad un trattamento su larga scala, quindi non si ritiene per il momento che possa rientrare nell'obbligatorietà di condurre la valutazione di impatto.

10. PROCEDURE

10.1. Procedura per la designazione del Responsabile del trattamento

La designazione dei Responsabili del trattamento dei dati personali viene effettuata in modo formale dal Titolare del trattamento (Legale Rappresentante) attraverso una lettera di nomina ("Atto di nomina a Responsabile del trattamento dei dati personali") sottoscritta per accettazione.

La validità della nomina cessa esclusivamente a fronte di revoca formale da parte del Legale Rappresentante o in caso di dimissioni del Responsabile del trattamento.

Le nomine dei responsabili esterni sono sia effettuate in modo formale dal Titolare del trattamento sia indicate nei contratti di outsourcing.

10.2. Procedura per la designazione degli incaricati dei trattamenti

La designazione degli Incaricati del trattamento dei dati personali (Personale Operativo) viene effettuata in modo formale dal Titolare del trattamento, attraverso una lettera di nomina ("Atto di nomina a Incaricato del trattamento dei dati personali") sottoscritta per accettazione ricevuta dall'incaricato.

La nomina viene effettuata all'atto dell'inserimento in azienda della persona e viene modificata e riemessa in caso di cambio di funzione o mansione e comunque in tutti i casi in cui è necessaria una modifica alle tipologie di trattamenti per i quali la persona viene incaricata.

Oltre tali casi di variazioni, la validità della nomina cessa esclusivamente a fronte di revoca formale da parte della Responsabile del trattamento o in caso di dimissioni dell'incaricato.

Sono previste anche delle nomine temporanee legata a progetti che coinvolgono collaboratori o outsourcer che hanno necessità di trattare dati personali HOSPITALIA SRL in relazione alle finalità del progetto/collaborazione.

10.3. Procedura per i diritti dell'interessato

1. Così come indicato nell'informativa predisposta dal Titolare del trattamento, ogni interessato, in quanto tale, ha i diritti di cui all'art. 7 Codice Privacy e art. 15 GDPR e precisamente i diritti di:

   i. ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;

   ii. ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2 Codice Privacy e art. 3, comma 1, GDPR; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;

   iii. ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco 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 successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

iv. opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che La riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, mediante l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore mediante e-mail e/o mediante modalità di marketing tradizionali mediante telefono e/o posta cartacea. Si fa presente che il diritto di opposizione dell'interessato, esposto al precedente punto b), per finalità di marketing diretto mediante modalità automatizzate si estende a quelle tradizionali e che comunque resta salva la possibilità per l'interessato di esercitare il diritto di opposizione anche solo in parte. Pertanto, l'interessato può decidere di ricevere solo comunicazioni mediante modalità tradizionali ovvero solo comunicazioni automatizzate oppure nessuna delle due tipologie di comunicazione. Ove applicabili, ha altresì i diritti di cui agli artt. 16-21 GDPR (Diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione), nonché il diritto di reclamo all'Autorità Garante.

2. L'interessato potrà in qualsiasi momento esercitare i diritti inviando:

   - una raccomandata a.r.;
   - una e-mail all'indirizzo email e/o pec.

3. Il Titolare del trattamento deve inviare risposta scritta all'interessato senza ingiustificato ritardo e al più tardi entro un mese.

4. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero di richieste. Il Titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

5. Ove l'interessato abbia inviato la richiesta tramite mezzi elettronici, le informazioni devono essere fornite tramite mezzi elettronici, fatto salvo diversa indicazione dell'interessato.

6. Nel caso in cui il Titolare del trattamento non ottemperasse alla richiesta dell'interessato, il titolare del trattamento deve informare l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi della non ottemperanza e della possibilità di proporre reclamo al Garante nazionale della Privacy e di proporre ricorso giurisdizionale.

7. Il Titolare del trattamento deve fornire le informazioni a titolo gratuito, fatto salvo quanto indicato al punto successivo.

8. Se le richieste dell'interessato fossero manifestatamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare del trattamento può:

   a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta;

   b) rifiutare di soddisfare la richiesta. Incombe al Titolare del trattamento l'onere di dimostrare il carattere manifestatamente infondato o eccessivo della richiesta.

9. Qualora il Titolare del trattamento nutrisse dubbi sull'identità della persona fisica che presenta la richiesta, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

10.4. Procedura gestione data breach

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 (GARANTE PRIVACY) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, sarà corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

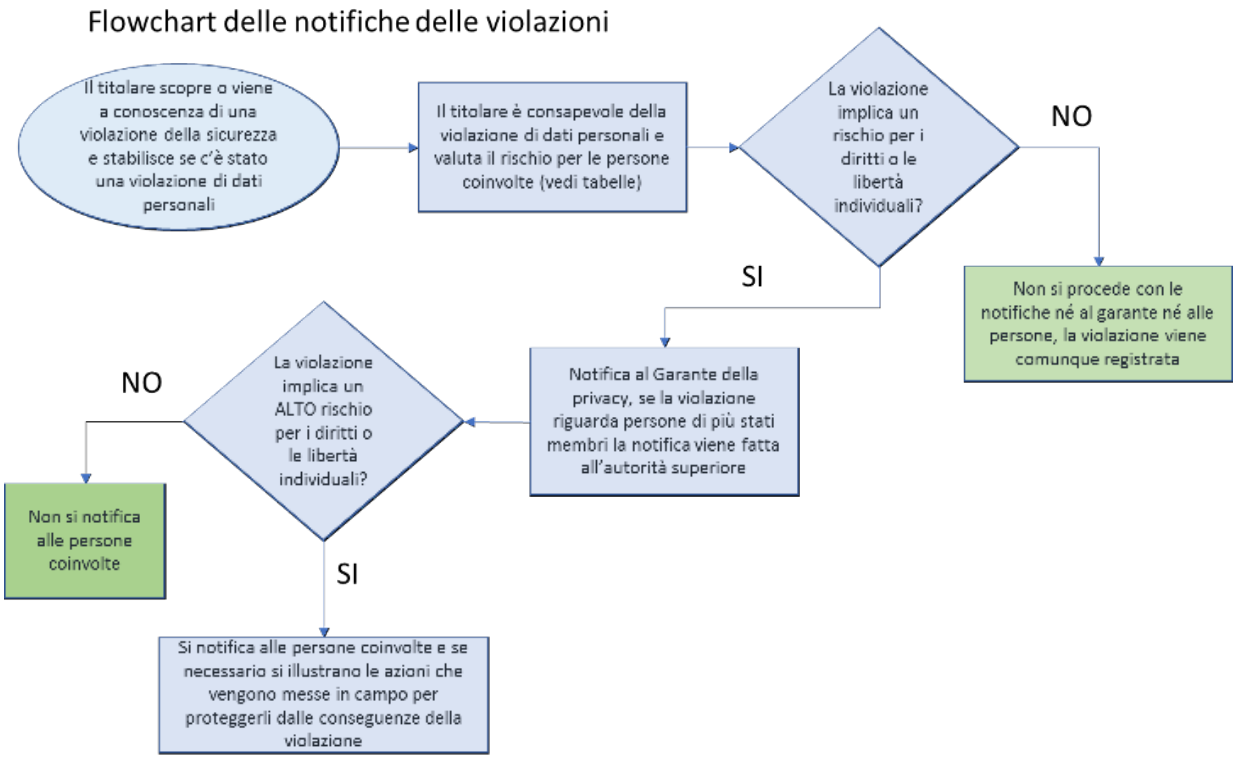
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

I seguenti diagrammi di flusso e tabelle correlate illustrano nei dettagli le procedure e i criteri che vengono seguiti.



Data Breach - caso	Notifica al Garante della Privacy	Notifica alle persone coinvolte	Note
Un titolare del trattamento ha archiviato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante una intrusione.	No	No	
Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono esfiltrati.	Si vedi il flowchart	Si vedi il flowchart, la notifica avviene in accordo con i suggerimenti del Garante	
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento comporta che i clienti non sono in grado di chiamare il titolare del trattamento e accedere ai loro record.	No	No	Questa non è una violazione soggetta a notifica, ma è comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. I registri appropriati devono essere conservati dal titolare del trattamento.

Data Breach - caso	Notifica al Garante della Privacy	Notifica alle persone coinvolte	Note
Un titolare del trattamento subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non vi erano altri malware presenti nel sistema.	Si, riferire all'autorità di vigilanza, se vi sono probabili conseguenze per gli individui in quanto si tratta di una perdita di disponibilità.	Si, riferire ai singoli, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati. La notifica avviene in accordo con i suggerimenti del Garante	Se fosse disponibile una copia di riserva e i dati potessero essere ripristinati in tempo utile, ciò non dovrebbe essere segnalato all'autorità di vigilanza o ai singoli in quanto non vi sarebbe stata alcuna perdita permanente di disponibilità o riservatezza. Tuttavia, se l'autorità di vigilanza è venuta a conoscenza dell'incidente con altri mezzi, può prendere in considerazione un'indagine per valutare la conformità ai requisiti di sicurezza più ampi dell'articolo 32.
Un titolare del trattamento gestisce un e-commerce e ha clienti in più Stati membri. Il mercato subisce un attacco informatico e nomi utente, password e cronologia degli acquisti sono pubblicati online dall'attaccante.	Segnalare all'autorità di vigilanza capofila se comporta l'elaborazione transfrontaliera.	Si se può produrre gravi rischi.. La notifica avviene in accordo con i suggerimenti del Garante	Il titolare del trattamento dovrebbe agire, ad es. forzando il ripristino della password degli account interessati, nonché altri passaggi per mitigare il rischio. Il responsabile del trattamento dovrebbe anche considerare qualsiasi altro obbligo di notifica, ad es. sotto la direttiva NIS come fornitore di servizi digitali.
Una società di hosting di siti Web che agisce come un elaboratore di dati identifica un errore nel codice che controlla l'autorizzazione dell'utente. L'effetto del difetto indica che ogni utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In qualità di elaboratore di dati, la società di hosting del sito web deve notificare i client interessati (i responsabili del trattamento) senza indebito ritardo. Supponendo che la società di hosting del sito web abbia condotto la propria indagine, i responsabili del trattamento interessati dovrebbero essere ragionevolmente fiduciosi sul fatto che	No, se non ci sono probabili rischi elevati per le persone.	La società di hosting del sito web (elaboratore dei dati) deve considerare qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS come fornitore di servizi digitali). Se non vi è alcuna prova che tale vulnerabilità sia sfruttata con uno dei suoi responsabili del trattamento, una violazione notificabile potrebbe non essersi verificata, ma potrebbe essere verosimilmente registrabile o essere oggetto di non

Data Breach - caso	Notifica al Garante della Privacy	Notifica alle persone coinvolte	Note
	ognuno abbia subito una violazione e quindi è probabile che venga considerato come "preso coscienza" una volta che sono stati notificati dalla società di hosting (l'elaboratore dei dati). Il responsabile del trattamento deve quindi informare l'autorità di vigilanza.		conformità ai sensi dell'articolo 32.
I dati personali di un gran numero di individui vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.	Si, segnalare all'autorità di vigilanza	Si, riferire agli individui in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze. Le informazioni devono essere inviate singolarmente	Il mail server ha un limite di invii contemporanei, meno di 100. Le applicazioni sono settate per invii individuali
Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sila notifica all'autorità di vigilanza può essere obbligatoria se un numero elevato di persone è interessato, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la posta contiene le password iniziali).	Si, riferire agli individui in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato solo un numero esiguo di indirizzi e-mail. Il mail server ha un limite di invii contemporanei, meno di 100. Le applicazioni sono settate per invii individuali

TABELLA IN CUI PER I DATI PERSONALI E PER I TIPI DI VIOLAZIONE (DISTRUZIONE, PERDITA O DANNEGGIAMENTO ACCIDENTALE, ACCESSO NON AUTORIZZATO, FURTO) SI STABLISCE A CHI NOTIFICARE (GARANTE O GARANTE + PERSONA COINVOLTA) IN MANIERA INDIVIDUALE O PUBBLICA – SITO-NEWSLETTER

Tipo di dato coinvolto nel data breach	distruzione	perdita	danneggiamento	furto	accesso non autorizzato
cod. 01 dati personali dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;	no	No	No	No	No
cod. 02 dati personali del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 03 dati personali dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati all'Azienda, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 04 dati personali di terzi, forniti dai clienti per l'espletamento degli incarichi affidati all'Azienda, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari;	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 05 dati personali dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 06 dati personali di altre Aziende e professionisti cui l'Azienda affida incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria;	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 07 dati particolari del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o l'adesione ad organizzazioni sindacali;	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 8 dati particolari dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati all'Azienda, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico (*);	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui
cod. 9 dati particolari dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati all'Azienda, idonei a rivelare lo stato di salute (*);	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui

cod. 10 dati particolari di clienti o terzi, comunque afferenti la vita sessuale (*).	si garante no individuali	si garante no individuali	si garante no individuali	Si garante si individui	Si garante si individui

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Nel caso in cui i SERVIZI WEB fossero TEMPORANEAMENTE NON DISPONIBLI DIVENTANO OGGETTO DI NOTIFICA se la non disponibilità supera il TEMPO LIMITE di 3 giorni solari consecutivi

REGISTRAZIONE NON CONFORMITA' E AZIONI CORRETTIVE

Viene tenuta comunque traccia dei data breach anche se non notificati al garante, attraverso la registrazione di un rapporto di non conformità e della conseguente azione correttiva.

11. FORMAZIONE DEL PERSONALE SULLA SICUREZZA DEI DATI PERSONALI

Gli incaricati ricevono una formazione di base finalizzata a minimizzare la probabilità di errori e a dare loro i riferimenti documentali e alcuni strumenti pratici di gestione

L'attuazione della formazione può essere programmata e articolata per profilo degli incaricati, in relazione alle specifiche esigenze, alla natura dei dati trattati, al tipo di rischi esistenti nelle aree e relativi trattamenti. Il piano di formazione ha i seguenti Obiettivi generali:

Conoscenza e consapevolezza del personale che effettua trattamenti di dati personali circa:

- rischi che interessano i dati;
- misure adottate e da adottare per prevenire eventi dannosi;
- profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- responsabilità che ne derivano e modalità per aggiornarsi sulle misure minime stabilite;
- garanzia necessaria del rispetto delle norme, delle procedure e delle istruzioni descritte.

La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati nonché quando intervengano cambiamenti di mansioni oppure vengano introdotti nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Titolare del trattamento dei dati personali deve redigere annualmente il piano di formazione del personale specificando le necessità di ulteriore formazione del personale stesso. Il Piano di formazione del personale deve essere predisposto per:

- informare gli incaricati del trattamento sui rischi che incombono sui dati nonché sulle misure disponibili per prevenire eventi dannosi;
- informare gli incaricati del trattamento sui profili della disciplina della protezione dei dati personali più rilevanti in rapporto alle relative attività;
- informare gli incaricati del trattamento sulle responsabilità che ne derivano;
- informare gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Qui di seguito si elencano i corsi di formazione aziendali già effettuati, in corso di svolgimento o pianificati per il futuro:

1) Formazione sul Regolamento Europeo 679/2016

Pianificazione: entro il 30/09/2020 Ore totali previste: 2

Descrizione completa: Formazione sui principi generali del nuovo Regolamento Europeo 679/2016 sulla protezione dei dati personali, a tutti gli incaricati e sulle procedure specifiche del sistema gestione privacy. Fornire le nozioni necessarie a applicare quando necessario le procedure: gestione diritti interessato, data breach, notifiche al Garante Privacy

Modalità: è stata consegnata una dispensa di illustrazione dei principi generali del nuovo Regolamento Europeo sulla Privacy e le buone prassi da applicare per garantire il livello di sicurezza dei dati definito dal Titolare del trattamento.

Destinatari: tutti gli incaricati

12. VERIFICA PERIODICA SUL RISPETTO DELLE PRESCRIZIONI DI SICUREZZA

12.1. Procedura per il controllo e la verifica delle prescrizioni relative alla sicurezza

il Titolare del trattamento ha l'onere di vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle proprie istruzioni e delle disposizioni.

Controllo operativo

- i responsabili aziendali hanno la responsabilità di tenere sotto controllo l'applicazione e l'adeguatezza delle prescrizioni per la sicurezza nell'ambito della propria funzione, anche per quanto riguarda i trattamenti affidati ad entità esterne. Forniscono al Titolare del trattamento le informazioni in merito e la segnalazione di ogni eventuale anomalia o problema in relazione alla sicurezza;
- il Titolare del trattamento verifica almeno annualmente lo stato, l'applicazione e l'adeguatezza delle prescrizioni del presente Manuale rispetto alla riduzione dei rischi e degli incidenti relativi alla sicurezza dei dati personali (rif. Allegato 2).
- Le informazioni fornite includono i risultati delle periodiche verifiche interne nonché di quelle ai fornitori ai quali sono affidati trattamenti di dati per conto dell'Azienda;
- il Titolare del Trattamento definisce le azioni correttive e di miglioramento da intraprendere relativamente alla sicurezza dei dati personali.
- il Titolare del Trattamento stabilisce la programmazione delle verifiche interne ed eventualmente verso i fornitori ai quali sono affidati trattamenti (laddove applicabili in base agli accordi contrattuali).

Qui di seguito si gli audit del sistema gestione privacy già effettuati, in corso di svolgimento o pianificati per il futuro:

1) Audit e riesame generale sul sistema di gestione privacy

Data di inizio prevista: 30/03/2021, e successivamente con cadenza annuale.

Obiettivi: Verificare che i requisiti definiti dal Regolamento Europeo 679/2016 sulla gestione dei dati personali siano correttamente applicati. Verificare che gli strumenti informatici e tecnologici applicati per garantire la sicurezza delle informazioni siano aggiornati e sufficienti.

13. ALLEGATI

Allegato 1: elenco Responsabili e incaricati al trattamento

ALLEGATO 1 – Tabelle Responsabili e incaricati al trattamento

1.1. Tabella riassuntiva Responsabili Trattamento

RAGIONE SOCIALE	DESCRIZIONE
PEA MARZIA, Via Santa Maria Della Rosa N. 23, 25012 Calvisano (bS), Codice Fiscale PEAMRZ74P62B157H. Consulente del lavoro iscritto al n. 862 ordine consulenti provincia di Brescia	Consulente lavoro
BRESCIA CONSULTING SRL, Via terranova 6, 25086 Rezzato (BS) P.IVA 03332270176.	CED (calcolo e stampa buste paga)
STUDIO BIANCHI, Via Giuseppe Sirtori 5/a, 37128 Verona, P.IVA 00153550231	Contabilità e adempimenti fiscali
SAFETY GROUP SRL, Via Labiena, 153, 21014 Laveno Mombello (VA), Part. IVA 03530040132 – Geom. Matteo Davide Sarcletti	RSPP e consulente SSL
CYBERIA INFORMATICA, Via Roma 57, Desenzano del Garda (BS), P.IVA 02795270988	Tecnico informatico
UNIVERSIIS – SOCIETA' COOPERATIVA SOCIALE – Via Cividina 41/A, 33100 Udine, P.IVA 01818390302	Prestazioni di servizi socio-sanitario-assistenziali

1.2. Tabella riassuntiva Incaricati Trattamento

NOME	DESCRIZIONE
CRISTIANO CASTELNOVO	Responsabile RSA (Trattamento di tutti i dati)