Documento Operativo Privacy

Indice

1. Parte prima: Introduzione generale al documento

Il presente documento è uno strumento di applicazione del nuovo **Regolamento Europeo n. 2016/679**, anche conosciuto come **"RGPD" e** del vigente **D.lgs. 30 giugno 2003, n. 196**(cosiddetto "Codice sulla Privacy" come novellato dal **D.lgs. 10 agosto 2018 n. 101**) nell'ambito dell'organizzazione della Casa Alloggio Don Luigi, .

A far data dal 25 maggio 2018 ha trovato infatti diretta ed immediata applicazione, sul territorio nazionale, il nuovo Regolamento Europeo n. 2016/679 (così detto RGPD ossia "*General Data Protection Regulation*") sulla Privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Ciò ha comportato l'adeguamento delle disposizioni legislative nazionali di cui al previgente Codice della Privacy (D.lgs. n.196/2003) al RGPD, con il D.lgs. n. 101 del 10 agosto 2018 di adeguamento al RGPD; le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali rimangono applicabili solo in quanto compatibili con la nuova normativa Privacy.

Il presente documento si rende necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di fonte europea che nazionale in tema di trattamento dei dati personali, al fine darne collocazione sistematica nel contesto in cui la Casa alloggio Don Luigi si trova a operare.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della **"responsabilizzazione" (accountability** nell'accezione inglese**)** che pone a carico al Titolare del trattamento dei dati l'onere di valutare il grado di tutele adeguato ai propri trattamenti e l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (**principio della "conformità" o compliance** nell'accezione inglese); vi è quindi l'obbligo

di porre in essere comportamenti pro-attivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE.

Nell'ottica del Legislatore europeo, quindi, in materia di privacy, ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli stesso risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto verso l'esterno e all'Autorità Garante per la protezione del dati personali.

Ciò premesso, questo documento sarà disponibile presso la Casa alloggio Don Luigi unitamente a tutta la documentazione adottata in conformità al RGPD.

Il documento operativo privacy adottato dalla Casa alloggio Don Luigi in attuazione del principio europeo dell'accountability, sarà a breve interamente fruibile sul sito internet della Cooperativa Roma Solidarietà nell'area dedicata alla Casa alloggio Don Luigi nell'apposita sezione denominata "*Privacy*".
La pagina, ora in completamento, conterrà i nuovi atti e le nuove modulistiche che, man mano, verranno approvati, così come gli aggiornamenti e le revisioni dei documenti esistenti.
Obiettivo di questa Struttura è infatti quello di dotarsi di un sistema organizzativo efficace e trasparente, che sia immediatamente fruibile e che risponda alle esigenze concrete e quotidiane dei propri operatori ed utenti.

1.1. Premessa di carattere organizzativo

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente,

che si rivolge ad una struttura socio sanitaria, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo.

Per questi motivi la "cultura della privacy" deve diventare un vero e proprio elemento cardine dell'organizzazione che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, principalmente fra gli operatori della sanità. Solo con la conoscenza dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo, nel trattamento dei dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.

1.2 Scopo

Scopo del presente documento è definire il modello organizzativo per la gestione degli adempimenti in materia di protezione dei dati e degli interessati, avendo come riferimento il Regolamento UE 2016/679 sulla protezione dei dati personali, il vigente D.Lgs. n. 196/2003, cosiddetto "Codice sulla Privacy" come novellato dal D.lgs. 10 agosto 2018 n. 101e i provvedimenti emanati nel tempo dal Garante per la protezione dei dati personali.

In particolare, il documento regolamenta:

a) i **ruoli e le responsabilità** assegnate ai vari livelli gestionali, di controllo e operativi, al fine di garantire la corretta tenuta del predetto modello e, di conseguenza, la conformità alla normativa di riferimento;

b) le modalità per il rilascio delle necessarie **istruzioni** ai soggetti autorizzati, ai vari livelli, al trattamento dei dati personali;

c) gli strumenti per il **monitoraggio e controllo** del sistema, al fine di garantire il miglioramento continuo dello stesso e il mantenimento della conformità alla normativa

vigente.

1.3 Campo di applicazione

Il presente documento si applica a tutta la struttura residenziale, ai dipendenti e ai collaboratori. Campo d'applicazione della procedura sono tutte quelle attività che rientrano nella definizione di trattamento di dati personali di cui alla normativa applicabile.

In particolare, ai sensi dell'art. 4 del RGPD, con l'espressione "trattamento di dati personali" s'intende *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali*", pertanto rientrano in tale definizione:

la raccolta dei dati;

la registrazione dei dati, ovvero il loro inserimento su supporti elettronici o in formato cartaceo;

il processo di lavorazione che favorisca la fruibilità dei dati;

la conservazione dei dati;

l'adattamento o la modifica dei dati registrati in relazione a rettifiche o nuove acquisizioni;

l'estrazione, ipotesi specifica che rientra nell'ipotesi più generale dell'elaborazione;

la consultazione o l'uso;

la comunicazione dei dati ad uno o più soggetti determinati, in qualunque forma;

il raffronto o l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte fra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;

la limitazione;

la cancellazione;

la distruzione.

1.4. Definizioni

Come stabilito dall'articolo 4 del Regolamento Europeo n. 2016/679, le definizioni adottate sono le seguenti:

· «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia cartaceo o informatizzato (è opportuno specificare) o sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

· «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

· «**consenso dell'interessato**»: 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;

· «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome e cognome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica ,culturale o sociale;

· «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di 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;

· «**dati relativi alla 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; per le tipologie di "dati" sopra indicate, si fa rinvio, per la disciplina di dettaglio, alle disposizioni di cui al D.lgs. n. 101 del 2018 che ha novellato il D.lgs. n. 196/2003 *(vedasi, in particolare, il Titolo 1° della Parte 1^, rubricato "Disposizioni generali").*

· «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

· «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

· «**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 interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

· «**pseudonimizzazione**»: 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;

· «**terzo**»: 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;

· «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

· «**violazione dei dati personali**»: 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.

Parte seconda – Le figure individuate dal RGPD

2.1. TITOLARE del Trattamento

Il **"Titolare"** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della Privacy, **è la Cooperativa Roma Solidarietà, promossa dalla Caritas di Roma** nella persona del suo Direttore Giustino Trincia, con sede in Roma, in Via Casilina Vecchia 19 cf: 05146971006.

Il Titolare, avvalendosi della supervisione e collaborazione del **DPO – Responsabile della Protezione dei Dati** provvede:

· a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;

· a nominare i *"Responsabili esterni"* del trattamento, ossia i soggetti esterni alla struttura aziendale che, nell'esecuzione di un servizio a favore del Titolare, trattano, per conto di quest'ultima, i dati personali in titolarità della stessa. Il Titolare ha la responsabilità di individuare al riguardo soggetti che presentino garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate

· a nominare *gli Incaricati del trattamento dei dati personali,* impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;

· a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

· a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

2.2. Data Protection Officer

Il DPO risulta essere un supervisore indipendente a garanzia, per i soggetti interessati al Trattamento. Esso è una figura a presidio della legalità, punto di riferimento nella realtà organizzativa e per l'Authority garante della Privacy. L'art. 37, paragrafo 1 del Regolamento RGPD sancisce le modalità di designazione del DPO sia in diversi ambiti:

in ambito *pubblico*, la nomina del DPO è sempre obbligatoria, fatta eccezione per l'autorità giurisdizionali in esercizio delle loro funzioni;

in ambito *privato*, la nomina del DPO è obbligatoria quando il Titolare effettua trattamenti regolari e sistematici, su larga scala, o inerenti a dati relativi a condanne penali o reati (come definito dall'art.10 del Regolamento).

L'articolo 39 del Regolamento sancisce i compiti assegnati al Responsabile della Protezione dei Dati, tra cui:

informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

cooperare con l'autorità di controllo;

fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

La CRS in qualità di Titolare del Trattamento,ha nominato il proprio DPO che è raggiungibile all'indirizzo di posta : privacy@caritasroma.it

2.3. Preposto alla Gestione delle Attività di Trattamento dei Dati

Il D.lgs. n. 196/2003, come novellato dal D.lgs. n. 101/2018 di armonizzazione del Codice italiano della Privacy alle novità del RGPD Europeo n. 2016/679, stabilisce, al nuovo articolo 2-quaterdecies, comma 1, che il Titolare può *"prevedere, sotto la propria responsabilità e*

nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità".

La Cooperativa Roma Solidarietà, in qualità di Titolare del trattamento di dati personali (cioè quale soggetto che determina le finalità e i mezzi dei trattamenti dei dati effettuati nel proprio ambito), è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione delle responsabilità al fine di assicurare il rispetto delle disposizioni vigenti in materia, e ciò sulla base del principio europeo di *accountability*, che prevede il coinvolgimento e la responsabilizzazione, ad ogni livello, delle strutture dell'azienda nel percorso di adeguamento ai precetti europei.

Per conoscere le figure professionali che operano all'interno della Casa alloggio " Don Luigi" è consultabile il funzionigramma -organigramma della struttura dove sono evidenziate le funzioni, le attività e le relative responsabilità del personale che, per il ruolo ricoperto ed in virtù dei poteri di organizzazione e gestione, risulta possedere i requisiti necessari per essere demandato anche all'esercizio delle funzioni di gestione, coordinamento e controllo delle attività di trattamento dei dati personali nonché dei correlati adempimenti previsti dal RGPD.

Tra le figure professionali incaricate del trattamento dei dati personali all'interno della Struttura abbiamo:

- 1 Coordinatore Organizzativo,
- 1 Medico : Responsabile Sanitario,
- 3 Infermieri Professionali.
- 7 OSS
- 1 Assistente Sociale
- 1 Psicologo

Preposto dal Titolare del Trattamento al rispetto delle prescrizioni in tema di privacy è il Coordinatore organizzativo che opera all'interno della struttura.

2.4. Incaricato (interno ed esterno) del trattamento dei dati

Ai fini del trattamento dei Dati Personali è possibile definire, all'interno di ogni struttura i soggetti interni da autorizzare a compiere operazioni di trattamento di dati personali contenuti in banche dati elettroniche o cartacee. Tali soggetti rivestono il ruolo di "*Incaricati al Trattamento*" per conto del Titolare del Trattamento. Quest'ultimo provvede alla definizione di un opportuno *obbligo legale di riservatezza* da sottoporre ai soggetti Autorizzati al Trattamento al fine di proteggere le informazioni trattate.

Al momento dell'ingresso in servizio quindi ogni *dipendente* (oltre che ad ogni *collaboratore*) viene quindi formalmente nominato quale "Incaricato al trattamento dei dati" ai sensi dell'art. 2-quaterdecies comma 2 del D.lgs. 196/2003 e del Regolamento UE 2016/679 , ricevendo anche le opportune "istruzioni operative" .

Incaricati esterni del trattamento dei dati

Tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito della struttura residenziale Casa Alloggio Don Luigi , pur non essendo dipendenti sono designati incaricati/autorizzati esterni.

Ci si riferisce, a mero titolo esemplificativo, al *personale volontario* che opera temporaneamente all'interno della Struttura in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato *(es. Associazione di volontariato o Istituto scolastico)*

Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli incaricati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Incaricati esterni, ovviamente, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività prevista dall'accordo o dalla convenzione.

Il Personale della Struttura Casa Alloggio "Don Luigi" CRS è così articolato:

2.5. Soggetti esterni

2.5.1 Responsabili "esterni" del Trattamento

Il Titolare, per effetto della conclusione ed esecuzione di specifici contratti, può demandare alcuni servizi che prevedono il trattamento di dati personali in sua titolarità a soggetti esterni alla propria struttura. In tali casi, i soggetti esterni sono nominati Responsabili "esterni" del trattamento, intesi, ai sensi dell'art. 4 del RGPD, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Il Responsabile "esterno" del trattamento deve essere nominato, con apposito contratto o atto giuridico. Secondo la normativa vigente, il Responsabile "esterno" è tenuto a presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Il Responsabile "esterno", inoltre, non può ricorrere ad un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare.

I trattamenti da parte di un Responsabile "esterno" del trattamento sono disciplinati da un contratto o da altro atto giuridico a norme del diritto dell'Unione o degli Stati membri; tale contratto tra il Titolare ed il Responsabile "esterno" del trattamento, oltre a vincolare a vicenda le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

2.5.2. Contitolari

Ai sensi dell'art. 26 del Regolamento, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In tali circostanze, il Regolamento richiede che tali soggetti determinino in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali derivanti dalla normativa applicabile, con particolare riguardo all'esercizio dei diritti dell'Interessato e le

rispettive funzioni di comunicazione delle informative di cui agli artt. 13 e 14 del Regolamento, salvo che le rispettive responsabilità siano già determinate per legge.
L'accordo di riparto costituisce un obbligo per i contitolari definendo i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
La contitolarità va ravvisata nella decisione condivisa delle finalità e dei conseguenti mezzi di trattamento tra Titolati distinti.

Parte terza: Disposizioni generali in materia di dati personali

In merito al trattamento dei dati personali, vengono messe in atto una serie disposizioni generali appositamente regolamentati dal RGPD, meglio descritti di seguito.

3.1. Principi applicabili al Trattamento dei Dati

Come stabilito dall'articolo 5 del Regolamento Europeo n. 2016/679, i dati personali sono:
· trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *(«***liceità, correttezza e trasparenza***»);*
· raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali *(«***limitazione della finalità***»);*
· adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati *(«***minimizzazione dei dati***»); a* tale proposito, il Regolamento UE ricalca i principi sostanziali di **"necessità, pertinenza, indispensabilità e non eccedenza"** (rispetto alle finalità del trattamento) contenuti nel D.lgs. n. 196/2003;

· esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati *(«***esattezza***»);*

· conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato *(«***limitazione della conservazione***»);*

· trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali *(«***integrità e riservatezza***»).*

Si precisa inoltre che:

il trattamento deve essere effettuato dagli *Incaricati del Trattamento* per gli scopi determinati nelle rispettive mansioni di lavoro;

i dati personali raccolti e/o trattati in violazione dei principi enunciati nei precedenti punti non possono essere ulteriormente oggetto di trattamento;

i dati personali oggetto del trattamento devono essere conservati per un periodo non eccedente a quello necessario per le finalità per cui gli stessi sono stati raccolti e trattati;

in nessun caso i dati personali possono essere utilizzati per scopi illeciti o incompatibili con i fini per i quali sono stati raccolti e registrati.

Parte quarta – Diritti dell'Interessato

4.1. Informativa al Trattamento dei Dati Personali

Il principio di trasparenza previsto dall'art. 5, par. 1, lett. a) del RGPD impone ai Titolari di informare gli interessati sui principali elementi del trattamento, al fine di renderli consapevoli sulle principali caratteristiche dello stesso.

Come stabilito dall'articolo 13 del Regolamento Europeo 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni:**

· l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;

· i dati di contatto del Responsabile della protezione dei dati (DPO);

· le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

· se il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi;

· gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

· ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il Titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni** necessarie per garantire un trattamento corretto e trasparente:

· il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

· l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;

· qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

· il diritto di proporre reclamo a un'autorità di controllo;

· se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

· l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione*, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il **periodo di conservazione** dei dati personali raccolti , i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

La Casa Alloggio Don Luigi ha affisso una informativa generale per tutti gli utenti dei servizi sanitari.

Alla luce dei principi suesposti, si rinvia ai vigenti moduli di "Informativa" (per utenti, lavoratori e fornitori) che verranno pubblicati sul sito web della CRS nell'apposita pagina web dedicata alla "Privacy".

4.2. Consenso al Trattamento dei Dati

Come stabilito dall'articolo 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche,* le *convinzioni religiose* o *filosofiche*, o *l'appartenenza sindacale*, nonché trattare *dati genetici, dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

Il RGPD stabilisce , pertanto ,un generale divieto di trattamenti dei dati relativi alla salute.

Le deroghe al divieto generale di trattare le cc.dd. "categorie particolari di dati", tra cui rientrano quelli sulla salute, sulla base delle quali è ammesso il trattamento di tali dati, sono

ora da individuarsi nell'art. 9 del Regolamento che elenca una serie di eccezioni che rendono lecito il trattamento e che, in ambito sanitario, sono riconducibili, in via generale, ai trattamenti necessari per:

a**) motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice;

b) **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);

c) **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** (di seguito "finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.

Con riferimento alla lettera c**) finalità di cura,** si precisa che i trattamenti per "finalità di cura", sulla base dell'art. 9, par. 2,lett. h) e par. 3 del RGPD, sono propriamente quelli effettuati **da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza**.

Diversamente dal passato, quindi, il professionista sanitario, soggetto al segreto professionale, non deve più richiedere il consenso del paziente per i trattamenti necessari alla prestazione sanitaria richiesta dall'interessato, indipendentemente dalla circostanza che operi in qualità di libero professionista (presso uno studio medico) ovvero all'interno di una struttura sanitaria pubblica o privata.

Con riferimento ai trattamenti in ambito sanitario che richiedono il consenso esplicito dell'interessato (art. 9, par. 2, lett. a)del RGPD, l'Autorità Garante per la protezione dei dati personali ha indicato, nel Provvedimento n.55 del 7 marzo 2019, a titolo esemplificativo:

· consultazione del Fascicolo Sanitario Elettronico (FSE);

· consegna del referto online;

· utilizzo di app mediche;

· fidelizzazione della clientela;

· finalità promozionali o commerciali;

· finalità elettorali;

· trattamenti effettuati attraverso il Dossier Sanitario Elettronico (DSE).

Ulteriori indicazioni sono state fornite con il Provvedimento n.146 del 5 giugno 2019 (Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101):

· trattamento di dati genetici per finalità di tutela di un soggetto terzo;

· lo svolgimento dei test genetici nell'ambito delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria;

· il trattamento effettuato mediante test genetici, compreso lo screening, a fini di ricerca o di ricongiungimento familiare;

· il trattamento effettuato per finalità di ricerca scientifica e statistica non previste dalla legge.

La Casa Alloggio Don Luigi non effettua alcuno dei trattamenti richiedente un consenso esplicito da parte dell'interessato.

Gli utenti della Casa alloggio Don Luigi sono soggetti affetti da HIV invitati alla Struttura residenziale da una Struttura pubblica "inviante" (CCTAD)

Posto quanto sopra, si fa integrale rinvio agli articoli 75, 2-sexies e 2-septies del D.lgs. n. 196/2003 (come novellato dal D.lgs.101/2018) contenenti specifiche disposizioni relative al trattamento delle categorie particolari di dati personali relative al trattamento dei dati genetici, biometrici e relativi alla salute. Con la nuova formulazione dell'articolo 75 del

D.lgs. n. 196/2003e s.m.i. è infatti chiarito che non occorre più il consenso per il trattamento dei dati per finalità di diagnosi e cura .

E' prevista la raccolta del consenso dell'interessato per procedere alla comunicazione al medico curante della patologia di cui il soggetto è affetto e per raccogliere l'eventuale consenso a fornire informazioni sanitarie a familiari dallo stesso paziente individuati.

4.3. Diritto di Accesso dell'Interessato

Come stabilito dall'articolo 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e in tal caso, di ottenere **l'accesso** ai dati personali e alle seguenti informazioni:

· le finalità del trattamento;

· le categorie di dati personali in questione;

· i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

· quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

· l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

· il diritto di proporre reclamo a un'autorità di controllo;

· qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

· l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un Paese terzo o a un'Organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.

Il Titolare del trattamento fornisce, se richiesto, una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per esercitare i diritti sopra citati, l'interessato può inviare richiesta al Titolare o al Responsabile della Protezione dei Dati personali.

L'interessato ha, altresì, diritto di presentare reclamo al Garante per la protezione dei dati personali. Il modulo per l'esercizio dei diritti può essere richiesto dallo stesso inviando una mail a: privacy@caritasroma.it

4.4. Diritto di Rettifica, Cancellazione e Limitazione

Come stabilito dagli articoli 16, 17 e 19 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento:

· la **rettifica** dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

· la **cancellazione** dei dati personali che lo riguardano senza ingiustificato ritardo, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento, e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;

Il diritto di cancellazione **non è applicabile** nella misura in cui il trattamento sia necessario:

- per l'adempimento di un obbligo legale che richiede il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità all'art.9, paragrafo 2, lettera h) e i) e dell'art. 9, paragrafo 3.

· il **diritto "all'oblio",** che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri Titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".

· Il **diritto alla limitazione**: è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** *(in attesa di tale rettifica da parte del Titolare)* **o si oppone al loro trattamento** *(in attesa della valutazione da parte del Titolare).*

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze *(consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).* Il diritto alla limitazione prevede che il dato personale sia **"contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Per esercitare i diritti sopra citati, l'interessato può inviare richiesta al Titolare o al Responsabile della Protezione dei Dati personali.

L'interessato ha, altresì, **diritto di presentare reclamo all'Autorità Garante** per la protezione dei dati personali.

4.5. Diritto alla Portabilità Dei Dati

Si tratta di uno dei nuovi diritti previsti dal Regolamento. Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica

ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del Titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE). L'esercizio di tale diritto non deve ledere i diritti e le libertà altrui Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'interessato, se tecnicamente possibile.

Il diritto alla portabilità dei dati non si applica ai trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare.

4.6. Diritto di Opposizione

Come stabilito dall'articolo 21 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

4.7. Processo Decisionale Automatizzato (Profilazione)

Come stabilito dall'articolo 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento

automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

· sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un Titolare del trattamento;

· sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato.

La Casa Alloggio Don Luigi non attua la profilazione.

Parte quinta – Sicurezza dei dati personali e misure di sicurezza di carattere organizzativo e tecnologico

5.1. Protezione dei Dati: Progettazione e Protezione

L'articolo 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese **"data protection by default and by design"**, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso",* secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

5.2. Registro Elettronico delle Attività di Trattamento

Tutti i Titolari e i Responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento UE.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano la Cooperativa Roma Solidarietà non può che avere forma elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

5.3. Protezione e Sicurezza dei Dati Personali

L'art. 5, par. 1, lett. f) del RGPD, stabilisce che i dati personali devono essere "*trattati in maniera da garantire* **un'adeguata sicurezza** *dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*". É importante notare che è l'intero trattamento a dover essere sicuro, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento.

Per questo motivo, non possono esistere dopo l'entrata in vigore del RGPD, obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati

MISURE	*DESCRIZIONE DEI RISCHI*	*TRATTAMENTI INTERESSATI*	*COME FUNZIONA E TEMPI DI APPLICAZIONE*
Istruzione agli incaricati		Tutti i trattamenti informatizzati	Ad ogni nuova assunzione e/o stipula di contratto vengono consegnate le istruzioni operative
Formazione		Tutti dipendenti/ tutti trattamenti	

Procedura di accesso mediante autenticazione/ credenziali personali	-furto delle credenziali di autenticazione -intercettazione di informazioni in rete -comportamenti sleali fraudolenti -disattenzione e/o incuria	Tutti i trattamenti informatizzati	Pianificazione di una procedura di allert periodico (ogni 3 mesi) per la modifica delle credenziali di autenticazione stabilita a giugno 2019
Presenza di antivirus	Virus informatici / codici malefici Non ferma attacchi informatici specifici	Tutti i trattamenti	Istallato su tutti i PC e i Mac per l'intercettazione di software malevoli
Presenza firewall hardware	Previene i più comuni attacchi informatici	Tutti i trattamenti	E' posto fisicamente tra il router e la rete locale (dove sono collegati tutti i p.c.)
Firewall centralino voip	Firewall interno del centralino		Permette accesso solo agli IP indicati in una whitelist
Protezione web	Previene navigazione su black siti(porno, droga, armi) - Spyware, motori anonymizer, proxy http		Analizza le richieste http e https e le filtra tramite un database di siti categorizzati
Piano di backup	-Eventi distruttivi dolosi o accidentali o dovuti a incuria - guasto ai sistemi complementari (es. impianto elettrico)	Tutta la gestione documentale/ archivi/ documenti presenti e elaborati in tutte le aree	La gestione documentale è memorizzata all'interno di un dispositivo NAS, il backup viene effettuato giornalmente in automatico dal programma di Backup installato e viene salvato su un dispositivo ulteriore che si trova in edificio separato rispetto a primo, per garantire la conservazione di almeno 1 NAS in caso di incidenti gravi alla struttura
Verifica della logistica degli apparecchi e del loro corretto posizionamento			
Disponibilità di estintori	Guasti ai sistemi complementari		Come da normativa

Misure di sicurezza:

L'articolo 32, paragrafo 1 del RGPD, ribadisce inoltre che le misure di sicurezza (tecniche ed organizzative) devono **"garantire un livello di sicurezza adeguato al rischio**" del trattamento.

Per ogni rischio occorre individuare la probabilità dell'evento, nonché la gravità dello stesso, in modo da stabilire le misure di sicurezza adeguate a mitigare il rischio.

All'interno del Registro del Trattamento sono evidenziati i singoli servizi della CRS e tutte le misure di sicurezza messe in campo dal Titolare del Trattamento per essere conforme alla normativa privacy.

5.4. Notifica di una Violazione dei Dati Personali all'Autorità di Controllo

Tutti i Titolari devono notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza *"senza ingiustificato ritardo"*, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda

considerando 85 del Regolamento UE); questa procedura va sotto il nome di **"Data Breach".** Pertanto,

la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per i diritti degli interessati che spetta, ancora una volta, al Titolare.

Il Titolare e il Responsabile della protezione dei dati della Struttura devono quindi essere informati tempestivamente dell'esistenza di una violazione (si veda le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE" adottate il 2/10/2017 ed emendate il 06/10/2018).

Il Titolare del trattamento, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Tra la modulistica è presente un modulo interno in caso venga accertata una violazione dei dati personali oggetto di trattamento.

5.5. Privacy audit

La previsione di audit, cioè adeguati controlli al fine di verificare l'applicazione della normativa e il rispetto delle istruzioni impartite è una misura di sicurezza perché consente al Titolare del Trattamento di intervenire in maniera diretta sul singolo servizio. Si tratta di una funzione affidata - nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione – al DPO coadiuvato dalla struttura di supporto.

Le attività di verifica sono di regola programmate e previamente comunicate ai soggetti coinvolti (salvo esigenze di audit a sorpresa) e sempre condotte alla presenza degli stessi.

Gli esiti delle verifiche, formalizzati in forma di audit report, sono:

- condivise con i soggetti auditi che possono richiedere, in ogni momento, chiarimenti;
- completate – in caso di rilevazione di Non conformità (NC) – dalla proposta di azioni correttive/preventive,

- formalizzate – immediatamente ove evidenzino NC, ovvero durante le relazioni periodiche.

5.6. Riesame del sistema di gestione della privacy

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di compliance alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate sia "testata regolarmente" (art. 32, par. 1, lett. d), del GDPR), il Sistema di gestione della Privacy delineato nel presente documento dovrà essere sottoposto a riesame, in occasione:

- dell'emanazione di nuove disposizioni normative, di pronunce giurisprudenziali, ovvero in relazione ad eventuali provvedimenti del Garante per la Protezione dei Dati di carattere cogente e/o interpretativo che abbiano un impatto sulla disciplina della protezione dei dati rilevante per l'ambito sanitario;
- di cambiamenti significativi della Struttura organizzativa che comportino la ridefinizione della governance interna, degli organigrammi e delle relative attività e responsabilità;
- in occasione dell'introduzione di nuovi significativi strumenti di gestione, rilevanti rispetto al trattamento di dati personali;
- nel caso di applicazione di sanzioni da parte dell'Autorità giudiziaria ovvero del Garante nella materia di cui trattasi.

Il riesame è istruito con la collaborazione del DPO, il quale redigerà, ove richiesto, apposita relazione in merito, tenuto conto delle informazioni disponibili quali desunte dalle proprie attività di supporto e di controllo.

5.7 Formazione e informazione interna

Nell'ottica di diffondere le conoscenze relative alla materia e di fornire adeguate istruzioni a tutto il personale Cooperativa Roma Solidarietà:

tutta la documentazione relativa al Sistema di gestione privacy è resa disponibile mediante condivisione in apposita cartella della intranet ovvero con forme equivalenti;

il funzionamento del Sistema di gestione privacy è presentato e descritto a tutti i Responsabili delle diverse aree in specifici incontri di condivisione, al fine di agevolarne la conoscenza e lo svolgimento dei ruoli e delle attività previste;

sono realizzati progetti formativi specifici:

- per i nuovi dipendenti, al loro ingresso nella Cooperativa
- per i vecchi dipendenti, con la previsione di sessioni di aggiornamento annuale.

Potranno inoltre essere pianificati ulteriori specifici percorsi o eventi secondo le modalità ritenute più idonee (seminari, workshop, convention, incontri frontali e altri), nei quali si terra conto anche delle specifiche esigenze comunicate dal Titolare.

L'organizzazione di tali percorsi ed eventuali specifiche azioni formative saranno progettati e gestiti operativamente dal Servizio Risorse Umane della CRS in accordo con il DPO.

.