



**REGOLAMENTO INTERNO**

**PER LA PROTEZIONE DEI DATI PERSONALI**

**POLICY PRIVACY INTERNA**

**Il presente Regolamento Interno è suscettibile di ulteriori aggiornamenti sulla base delle indicazioni del Garante Privacy e del Codice di condotta SMS Fimiv in fase di elaborazione.**

***Ultima versione Ottobre 2018***



## 1. Finalità

Il presente Regolamento stabilisce le politiche e le misure organizzative e procedurali per garantire che i Dati Personali

- a) siano acquisiti e trattati su idonea e pertinente base giuridica per scopi determinati, espliciti e legittimi;
- b) siano trattati solo per le finalità proprie della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ e in maniera non eccedente le predette finalità;
- c) siano trattati nel rispetto dei diritti e della dignità degli interessati;
- d) siano protetti dal rischio, anche solo potenziale, di distruzione, perdita, modificazione, rivelazione non autorizzata, accesso non autorizzato, non esattezza e non adeguatezza rispetto alle finalità per cui sono trattati.
- e) siano comunicati legittimamente all'interno e all'esterno della società.

### 1.1. Contitolari del trattamento.

Allorché la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ determini le finalità e la modalità del trattamento con altre persone fisiche o giuridiche, dovranno stabilire con queste accordi di contitolarità.

Nell'accordo con il Contitolare sono definite le responsabilità in merito all'osservanza degli obblighi derivanti dal presente Regolamento e dalla normativa vigente, con particolare riguardo all'esercizio dei diritti dell'interessato e in generale ai rapporti del titolare e del contitolare con l'interessato.

Indipendentemente dalle disposizioni dell'accordo della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ con i Contitolari, il titolare del trattamento o il Responsabile del trattamento assicura, per quanto nella sua materiale possibilità, l'esercizio dei propri diritti da parte degli interessati ed eventualmente segnalano al *Data Protection Officer* eventuali inadempienze del Contitolare.

## 2. RESPONSABILI DEL TRATTAMENTO.

I Responsabili del Trattamento devono assicurare che gli Incaricati del trattamento e chiunque sia sottoposto alla direzione dei Responsabili medesimi, osservino il presente Regolamento e la normativa vigente, ivi incluse le direttive delle Autorità competenti in materia di dati personali. I Responsabili assicurano altresì il raggiungimento e il mantenimento di un livello di protezione adeguato in relazione allo specifico o agli specifici trattamenti di dati personali, coordinando trasversalmente i soggetti coinvolti.



In particolare, ogni Responsabile del Trattamento , deve garantire:

- a) l'adozione di idonee misure per assicurare, nell'organizzazione delle prestazioni e dei servizi che comportano il trattamento di Dati Personali ed in relazione al predetto trattamento, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati;
- b) la compilazione e il costante aggiornamento del Registro dei Trattamenti;
- c) la correttezza, l'esattezza e la completezza di dati personali oggetto di trattamento sotto la sua responsabilità;
- d) l'esecuzione, in fase di progettazione di nuovi trattamenti, qualora ciò sia ritenuto necessario, di una valutazione di impatto e di rischio, conforme alle direttive stabilite nel presente Regolamento;
- e) la nomina con atto formale da adottarsi sul modello allegato delle persone incaricate del trattamento dei dati personali e che possono avere accesso agli stessi;
- f) che non siano trasmesse e non sia consentito l'accesso ai Dati Personali a soggetti non incaricati del loro trattamento in conformità al presente Regolamento;
- g) che siano trasmessi o sia consentito l'accesso ai dati personali trattati nell'ambito della propria area di competenza solo previa adozione di misure tecniche di protezione eventualmente stabilite nel presente Regolamento (quali, a titolo esemplificativo l'anonimizzazione dei Dati Personali) e salvo che la trasmissione o l'accesso ai dati sia consentita senza adozione di misure di protezione dal presente Regolamento, da istruzioni specifiche della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ o da norme imperative di legge;
- h) che gli incaricati del trattamento o chiunque operi sotto la direzione del Responsabile medesimo abbia ricevuto e riceva una formazione adeguata;
- i) la costante collaborazione con il *Data Protection Officer* in relazione ai compiti ad esso affidati in base la presente Regolamento.

## **2.1. Nomina di un responsabile esterno del trattamento.**

Alla nomina di Responsabili del Trattamento esterni alla SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ si provvede su richiesta del TITOLARE DEL TRATTAMENTO.

La nomina di un responsabile esterno deve essere contenuta in un contratto tra il TITOLARE così nominato e la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ.

Il contratto deve indicare e stabilire:



- a) la durata del trattamento;
- b) la natura e la finalità del trattamento;
- c) il tipo di dati personali e le categorie di interessati;
- d) gli obblighi e i diritti del responsabile.

Il contratto deve altresì prevedere l'impegno del Responsabile Esterno:

- a) a trattare i dati personali nel rispetto del presente Regolamento e seguendo le istruzioni specifiche e particolari della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ;
- b) a trattare i dati personali esclusivamente per le finalità previste dal contratto o dalla convenzione;
- c) a compilare e tenere aggiornato il registro dei trattamenti di della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ ovvero a tenerne uno proprio, purché conforme alle indicazioni del presente Regolamento, rendendolo accessibile alla società;
- d) a nominare i soggetti incaricati del trattamento;
- e) a garantire e documentare
  - a. l'adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio connesso al trattamento;
  - b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- f) a garantire i diritti degli interessati ovvero a provvedere direttamente a soddisfare eventuali richieste degli stessi che siano manifestazione di un diritto loro attribuito dalla normativa vigente;
- g) a cancellare o restituire alla SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ tutti i dati personali alla scadenza del contratto salvo che vi sia un obbligo stabilito da una disposizione inderogabile di legge che preveda la conservazione dei dati da parte del Responsabile esterno;
- h) a consentire le attività di audit, comprese le ispezioni, da parte della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ o da un altro soggetto da questo incaricato.



### 3. INCARICATI DEL TRATTAMENTO.

Ogni dipendente preposto ad un determinato servizio che implichi il trattamento di dati deve ricevere un incarico dal TITOLARE DEL TRATTAMENTO cui risponde sulla base del modello allegato.

Il TITOLARE DEL TRATTAMENTO deve verificare gli atti di incarico con cadenza annuale per eventuali adeguamenti riguardanti le fonti normative o regolamentari, le mutate esigenze, le modifiche procedurali, i mutamenti dei ruoli, le cessazioni dal servizio.

L'Incaricato deve attenersi al presente Regolamento e alle istruzioni impartite dal TITOLARE DEL TRATTAMENTO

Gli incaricati devono comunque assicurare che i dati personali:

- a) siano raccolti e registrati per scopi determinati, espliciti e legittimi, conformemente al consenso prestato dall'interessato o alle finalità coerenti con la diversa base giuridica del trattamento individuata dal presente Regolamento o a seguito di eventuale DPIA;
- b) esatti e, se necessario, aggiornati, pertinenti, completi, non eccedenti rispetto al conseguimento delle finalità per le quali il dato viene raccolto e, ove si tratti di dati sensibili, indispensabili rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- c) 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.

#### 3.1. Incaricati esterni del trattamento.

I soggetti che operano sotto la direzione di un **Responsabile esterno** nelle attività di trattamento dei dati personali di cui è titolare la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ devono essere da detto Responsabile nominati "soggetti designati" al trattamento.

#### 3.2. Responsabile della Protezione dei dati – Data Protection Officer (DPO).

Il Responsabile della protezione dei dati (DPO Data Protection Officer) ha il compito di supportare SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ con i seguenti compiti:

- raccolta di informazioni per individuare i trattamenti svolti;
- analisi e alla verifica dei trattamenti in termini di loro conformità alla normativa vigente ovvero alle istruzioni impartite dalla SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ ai Responsabili del Trattamento e da questi ultimi agli incaricati;



- attività di informazione, consulenza e indirizzo nei confronti del titolare e del responsabile;
- consulenza in caso di esercizio da parte degli interessati dei diritti loro riconosciuti dalla legge ovvero ricevere e gestire direttamente le predette richieste.
- gestione dei rapporti con le Autorità pubbliche di vigilanza nei modi e nei termini previsti dalla normativa vigente.

Il TITOLARE DEL TRATTAMENTO deve coinvolgere il *Data Protection Officer* fin dalla fase di progettazione di attività e processi che comportano il trattamento di dati personali.

Il TITOLARE DEL TRATTAMENTO presta la sua collaborazione al *Data Protection Officer* ovvero da istruzioni in tal senso agli Incaricati.

### **3.3. Monitoraggio**

Il *Data Protection Officer* avvalendosi delle strutture interne, collabora al costante monitoraggio dell'applicazione del presente Regolamento e riporta con cadenza annuale al vertice della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ mediante relazione sui seguenti aspetti:

- a) evoluzione del contesto interno ed esterno e monitoraggio sistematico dell'evoluzione del quadro normativo;
- b) valutazione di conformità di ogni nuova finalità di trattamento dei dati personali ovvero di ogni variazione delle finalità e delle modalità dei trattamenti esistenti;
- c) monitoraggio dell'evoluzione degli scenari di rischio in materia di protezione dei dati personali
- d) verifica dei singoli trattamenti al fine di determinare se sono svolti in conformità ai requisiti applicabili in base al presente Regolamento e alle DPIA eventualmente eseguite.

In ogni caso il *Data Protection Officer* assicura che con cadenza almeno annuale sia eseguita una verifica di conformità rispetto a quanto prescritto nel presente Regolamento.

### **4. REGISTRO DEI TRATTAMENTI**

La SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ istituisce il Registro dei Trattamenti. Il Registro è tenuto in formato elettronico mediante sistema che consenta di tenere traccia delle modifiche ad esso apportate.

La SOCIETÀ DI MUTUO SOCCORSO potrà utilizzare il Registro dei trattamenti come strumento di organizzazione nel trattamento dei Dati personali, come strumento di adeguato presidio dei rischi e di buona gestione dei rapporti con gli interessati.



Il registro del trattamento deve essere aggiornato al mutare di uno qualunque degli elementi sopra indicati.

Quando il trattamento è il medesimo viene registrato una sola volta

Nel caso in cui più trattamenti siano necessari per conseguire una identica finalità ovvero rientrino in procedimenti complessi, cui possono partecipare più Responsabili del trattamento, la registrazione è organizzata in un sistema di trattamenti e subtrattamenti.

### **5. VALUTAZIONE DI IMPATTO E DI RISCHIO (DPIA)**

Prima di inserire nel Registro un nuovo trattamento ovvero prima di registrare una modifica ad un trattamento esistente, soprattutto se prevede l'utilizzo di nuove tecnologie, l'incaricato, o se nominato, il Data Manager, deve verificare se il nuovo trattamento o la modifica a quello esistente comportino un rischio elevato per i diritti e le libertà degli interessati e sia dunque opportuno procedere con una valutazione di impatto e di rischio (DPIA). Per verificare se il nuovo trattamento necessita di una valutazione di rischio deve essere verificato se il trattamento comporta :

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e che riguardano ad esempio il rendimento professionale, la situazione professionale, la situazione economica, la salute, l'affidabilità;
- b) il trattamento, su larga scala, di categorie particolari e sensibili di dati;
- c) dati aventi carattere altamente personale;
- d) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
- e) match o combinazione di database e/o di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale;
- f) dati relativi a persone vulnerabili (es. minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- g) gli utilizzi innovativi o l'applicazione di nuove soluzioni tecnologiche o organizzative;
- h) trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

E' importante che questa valutazione preliminare sia trasmessa al DPO o all'Organismo di Vigilanza perché possa esprimere la propria opinione al riguardo.

Se eseguita, la DPIA deve contenere almeno:



- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione di probabilità che il trattamento pregiudichi uno o più diritti e libertà degli interessati;
- d) una valutazione sul livello di pregiudizio che il trattamento potrebbe arrecare;
- e) uno o più diritti e libertà degli interessati;
- f) l'identificazione delle soluzioni e misure per gestire e mitigare i rischi individuati, includendo misure di sicurezza e organizzative a garanzia della protezione dei Dati personali e della conformità alla normativa vigente.

La valutazione deve riguardare i seguenti elementi:

- a) descrizione del trattamento, che specifichi natura, oggetto, contesto, finalità del trattamento;
- b) categorie di Dati personali trattati;
- c) natura dei Dati personali trattati;
- d) necessità e proporzionalità dei trattamenti in relazione alle finalità (con conseguente esame ad es. della liceità del trattamento, della minimizzazione del trattamento e del rispetto delle finalità oggetto di informative);
- e) rischio per la sicurezza dei dati;
- f) rischi per i diritti e le libertà degli interessati;
- g) misure organizzative in essere per mitigare i rischi
- h) misure tecniche in essere per mitigare i rischi.

Sul modo di procedere alla DPIA è sempre opportuno consultarsi con il DPO ( se nominato o con l'Organismo di Vigilanza )

*L'appendice B allegato al Codice di Condotta Privacy riporta una metodologia semplificata di DPIA che potrà essere utilizzata in via ordinaria dalla Società, **che resta comunque libera di scegliere una diversa modalità.***

Gli esiti della valutazione devono essere formalizzati in un report finale finalizzato a riassumere il processo DPIA, le scelte compiute per mitigare il rischio e consentire la tracciabilità e documentabilità del processo stesso. Al Report devono essere allegate le osservazioni del Data Protection Officer.

Se i rischi rimangono probabili e alti deve sempre essere richiesto l'intervento dell'Autorità Garante per la protezione dei Dati personali.



## 6. ACQUISIZIONE DEI DATI PERSONALI.

Un dato personale è acquisito dalla SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ quando viene ricevuto da un incaricato del trattamento o da altro dipendente o collaboratore, in forma scritta (anche mediante mezzi informatici) o orale (anche mediante sistemi telefonici) ovvero quando viene acquisito senza intervento umano e viene archiviato su qualunque supporto che ne consenta il successivo trattamento a qualunque fine (web).

I dati personali sono acquisiti direttamente dall'interessato quando è l'interessato medesimo o chi ne abbia la rappresentanza a trasmetterli alla società, mentre i dati non sono acquisiti dall'interessato quando sono già in possesso della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ ovvero quando vengono forniti da un terzo.

### 6.1. Informativa.

**Il rilascio di una informazione conforme al presente Regolamento agli interessati è adempimento inderogabile qualunque sia la base giuridica utilizzata per il trattamento dei dati personali.**

**Il titolare del trattamento si deve assicurare che prima dell'acquisizione dei dati personali o contestualmente all'acquisizione degli stessi sia stata consegnata o comunque messa a disposizione degli interessati o di chi li rappresenta l'informativa sul trattamento dei dati personali.**

Il titolare del trattamento si assicura che l'informativa sia trasparente, intelligibile per l'interessato, facilmente accessibile e che sia scritta in un linguaggio chiaro e semplice.

Il titolare del trattamento sentito il *Data Protection Officer*, assicura la predisposizione dell'informativa privacy rispetto alle informazioni contenute nel Registro dei Trattamenti e con le prescrizioni del presente Regolamento. Nei trattamenti che richiedono l'espletamento di una DPIA l'informativa è redatta all'esito della stessa e secondo le indicazioni fornite nella medesima. **L'informativa è resa disponibile sul sito web della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ con link di accesso su tutte le pagine dello stesso.**

Gli incaricati su richiesta degli interessati devono sempre fornire indicazioni su dove reperire l'informativa estesa e, nei limiti in cui ciò sia ragionevolmente possibile, fornirla oralmente o consegnandone copia.

#### 6.1.1. Informativa in caso di contitolarità.

In caso di rapporti di contitolarità, salvo che l'accordo tra la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ e il Contitolare preveda

- a) che l'informativa sia resa da quest'ultimo;



- b) che il contitolare renda informativa separata per i trattamenti o parte di essi da questo posti in essere;

i contenuti dell'informativa sono resi anche con riferimento ai dati, ai trattamenti e alle finalità che ricadono in base agli accordi sotto la responsabilità del Contitolare.

In ogni caso, l'informativa contiene una descrizione sintetica dell'accordo ( o la specifica indicazione di come reperire l'accordo) tra la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ e il CONTITOLARE.

#### **6.1.2. Informativa in caso di acquisizione dei dati da soggetti terzi**

Qualora i dati siano acquisiti da terzi, Il titolare del trattamento prima di avviare il trattamento, deve verificare che sia stata fornita agli interessati l'informativa ovvero il link al sito da cui acquisirla.

In tali casi l'informativa deve anche indicare la fonte da cui sono stati acquisiti i dati personali anche nel caso in cui i dati provengano da fonti accessibili al pubblico.

Ove tale informativa non sia stata resa, Il titolare del trattamento deve provvedervi entro trenta giorni da quando i dati sono stati acquisiti.

#### **6.1.3. Informativa sull'utilizzo di cookies nel sito web**

L'informativa sull'utilizzo dei cookies deve immediatamente comparire in primo piano un banner di idonee dimensioni ossia di dimensioni tali da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che si sta visitando contenente le seguenti indicazioni:

- a. che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;
- b. che il sito consente anche l'invio di cookie "terze parti" (laddove ciò ovviamente accada);
- c. il link all'informativa estesa, ove vengono fornite indicazioni sull'uso dei cookie tecnici e analytics, viene data la possibilità di scegliere quali specifici cookie autorizzare;
- d. l'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione di qualunque cookie;
- e. l'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio, di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie.



Il banner, oltre a dover presentare dimensioni sufficienti a ospitare l'informativa, seppur breve, deve essere parte integrante dell'azione positiva nella quale si sostanzia la manifestazione del consenso dell'utente. Il superamento della presenza del banner al video deve essere possibile solo mediante un intervento attivo dell'utente. E' necessario in ogni caso che dell'avvenuta prestazione del consenso dell'utente sia tenuta traccia mediante apposito cookie tecnico.

La presenza di tale "documentazione" delle scelte dell'utente consente poi di non riproporre l'informativa breve alle successive visite del medesimo utente

All'interno di tale informativa, deve essere inserito anche il link aggiornato alle informative e ai moduli di consenso delle terze parti con le quali ha stipulato accordi per l'installazione di cookie tramite il proprio sito.

## **7. BASI GIURIDICHE DEL TRATTAMENTO**

Previo rilascio dell'informativa, i dati personali possono essere raccolti e trattati dalla SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ al ricorrere di una delle seguenti circostanze:

- a) l'interessato o chi ne la rappresentanza ha espresso il consenso al trattamento dei dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;
- c) il trattamento è necessario per adempiere un obbligo legale;
- d) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Nel caso di dati idonei rivelare

- a) l'origine razziale o etnica,
- b) le opinioni politiche,
- c) l'appartenenza sindacale,
- d) dati relativi alla salute

sono valide basi giuridiche per il trattamento:

- a) il consenso dell'interessato o chi ne ha la rappresentanza, purché si tratti di consenso esplicito e per una o più finalità specifiche;



- b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- c) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- d) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- e) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale;

Il trattamento dei dati deve essere fondato in via ordinaria e prioritaria sul consenso. L'utilizzo di diverse basi giuridiche deve essere previsto dal presente Regolamento ovvero essere indicato, eventualmente, a seguito di DPIA. Nel caso sia già stata eseguita una DPIA su fattispecie analoga può procedersi su base giuridica diversa dal consenso previo parere del *Data Protection Officer* (se nominato).

### **7.1. Esclusione del consenso.**

I dati personali possono essere raccolti e trattati i senza necessità di consenso dell'interessato:

- a) nella gestione del rapporto di lavoro trovando il trattamento fondamento nel relativo contratto e purché sia a questo allegata la relativa informativa o la stessa sia stata comunicata al dipendente in caso di nuovo trattamento.
- b) per la difesa in giudizio e di fronte ad autorità amministrative in procedimenti sanzionatori o comunque afflittivi.

### **7.2. Modalità di raccolta del consenso presso i locali della società.**

Gli incaricati che in ragione dell'organizzazione interna devono raccogliere il consenso al trattamento dei dati sono tenuti a procedere secondo le seguenti modalità:

- a) devono verificare l'identità dell'interessato chiedendogli di esibire un documento di riconoscimento in corso di validità e riscontrare la corrispondenza dei dati con quanto dichiarato nel modello.
- b) prima di consegnare il modulo per il consenso l'incaricato deve verificare che lo stesso non risulti precompilato in nessuna sua parte;
- c) nel caso gli interessati siano minori, gli incaricati devono verificare che il modello per la raccolta del consenso sia stato debitamente compilato nella parte in cui chi presta il consenso debba dichiarare di essere esercente la potestà genitoriale o un suo delegato;
- d) in ogni caso gli incaricati devono verificare che sia stata sottoscritta la dichiarazione di presa visione della documentazione;



- e) il consenso deve essere rilasciato in forma scritta utilizzando l'apposito modulo predisposto dalla SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ e deve riguardare in maniera separata e distinta il trattamento dei dati personali;
- f) l'incaricato del trattamento deve assicurare la conservazione del modulo relativo al consenso per tutta la durata del trattamento.

### **7.3. Il consenso per via telematica in relazione ai servizi prestati dalla società.**

L'accesso ai servizi on-line se offerti deve essere consentito solo a utenti registrati.

La registrazione deve poter avvenire solo a titolo personale mediante emissione di codici identificativi e chiavi di accesso univoche e deve essere confermata mediante procedura che preveda l'invio di una mail all'indirizzo dichiarato nel form di registrazione dell'interessato con indicazione di un link.

Al fine di assicurare una corretta acquisizione del consenso:

- a) nessuna delle caselle deve essere preimpostata;
- b) l'interessato deve aver selezionato la casella di presa visione dell'informativa che deve essere distinta da quella per la prestazione del consenso;
- c) le caselle del consenso devono avere funzione esclusiva e devono essere distinte per ogni trattamento avente finalità diversa;
- d) la mancata prestazione del consenso deve impedire l'accesso al servizio on line esclusivamente se è omesso in relazione ai dati che sono necessari all'esecuzione del servizio medesimo.

## **8. PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA.**

### **8.1. Politiche generali per il trattamento di dati in forma cartacea.**

Le Società di mutuo soccorso, anche a seguito dell'esecuzione di una valutazione di impatto e di rischio relativamente alla gestione dei dati idonei a rivelare lo stato di salute, compatibilmente con le risorse finanziarie disponibili per ciascuna, dovrebbero adottare una progressiva digitalizzazione dei propri archivi correnti.

Anche a prescindere dall'esecuzione di una valutazione di impatto e di rischio il TITOLARE DEL TRATTAMENTO deve definire le politiche per la gestione di dati attraverso strumenti informatici sulla base della dotazione informatica della Società, di ogni aspetto relativo all'organizzazione e alla logistica e dell'esistenza di piattaforme condivise anche in ragione di rapporti di contitolarità.



Nell'appendice A allegato al CODICE DI CONDOTTA PRIVACY sono fornite le linee guida contenenti le azioni suggerite, non vincolanti, per una corretta gestione dei sistemi, degli applicativi e delle dotazioni informatiche.

L'archiviazione e la catalogazione dei documenti deve essere organizzata in maniera da permettere la pronta reperibilità e l'identificazione dell'interessato, al fine di consentire l'esercizio dei propri diritti da parte di quest'ultimo.

Gli atti e i documenti contenenti dati personali, affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, devono essere utilizzati assicurandosi che agli stessi non abbia accesso altro personale della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ non coinvolto nel trattamento, ovvero a visitatori e terze parti.

Le singole fasi di lavoro e la condotta da osservare devono evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

### **9. POLITICHE GENERALI PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI**

Nella gestione dei dati attraverso strumenti informatici il TITOLARE DEL TRATTAMENTO si atterrà alle linee guida di cui all'APPENDICE A del CODICE DI CONDOTTA PRIVACY

Nello specifico si attiverà per

- a) predisporre un inventario degli asset

Il perimetro di sicurezza fisica, con particolare riferimento al centro di elaborazione dati, deve considerare i seguenti aspetti:

-devono essere previste barriere fisiche per impedire l'accesso fisico non autorizzato al centro di elaborazione dei dati;

Il controllo di accesso fisico, con particolare riferimento al centro di elaborazione dati, deve considerare i seguenti aspetti:

- i diritti di accesso alle aree di sicurezza dovrebbero essere rivisti, aggiornati e revocati in caso di necessità.

### **10. POLITICHE GENERALI RELATIVE ALLA PROTEZIONE DEI DATI SENSIBILI E ALLA CONDIVISIONE ALL'INTERNO DELLA SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ**

Il titolare del trattamento e gli incaricati del trattamento che trattino dati idonei rivelare:



- a) l'origine razziale o etnica,
- b) le opinioni politiche,
- c) l'appartenenza sindacale,
- d) dati relativi alla salute

possono

- (i) condividerli
- (ii) impiegarli per un trattamento diverso da quello per il quale sono stati originariamente acquisiti
- (iii) conservarli oltre il termine di conservazione del trattamento e in assenza di possibili o probabili, ulteriori futuri trattamenti,

**solo se, alternativamente:**

- a) il trattamento ulteriore senza applicazione delle misure di protezione è stato oggetto di consenso da parte dell'interessato.
- b) i dati vengono sottoposti a procedure di anonimizzazione o pseudonimizzazione;
- c) il dato deve essere trasferito alla funzione ricevente per consentirle di svolgere un trattamento che ha una base giuridica diversa dal consenso, come risultante dal Registro dei Trattamenti.

**10.1. Scelta delle misure di protezione.**

La scelta della tipologia di protezione dei dati di cui al punto b) compete al TITOLARE DEL TRATTAMENTO della funzione trasmittente in ragione della migliore organizzazione del proprio servizio e sentito il *Data Protection Officer*

**10.2. Anonimizzazione.**

Gli incaricati devono intervenire sui dati personali in modo da rendere impossibile l'identificazione degli stessi o la deduzione dell'identità dell'interessato anche a chi abbia avuto originariamente accesso ai dati personali.

Nella condivisione dei documenti tra funzioni o con Responsabili esterni del Trattamento e in ogni caso di trattamenti futuri possibili o probabili, deve essere usato in via preferenziale un sistema di Privacy differenziale in forza della quale una copia dei dati originali rimane presso la funzione trasmittente mentre il ricevente acquisisce solo dati anonimi.

Le tecniche di anonimizzazione, da utilizzarsi anche cumulativamente agendo sui dati identificativi dell'interessato e sui dati a partire dai quali possa essere ricostruita l'identità dell'interessato, considerando il grado di rischio e l'uso previsto dei dati, possono essere le seguenti.

- sostituzione delle directory mediante modifica del nome delle persone integrate nei dati;



- scrambling mediante miscelazione o l'offuscamento delle lettere;
- mascheramento sostituzione di una parte dei dati con caratteri casuali o altri dati;
- sfocatura: un'approssimazione dei valori dei dati per rendere il loro significato.

### **10.3. Pseudonimizzazione.**

il TITOLARE DEL TRATTAMENTO ove non possa procedere alla anonimizzazione dei dati, in ragione della necessità di dover reidentificare l'interessato per possibili o probabili trattamenti futuri, procede a sostituire i campi di identificazione all'interno di una registrazione di dati con uno o più identificatori artificiali o pseudonimi.

### **10.4. Misure tecniche di protezione.**

I sistemi e i programmi informatici a supporto degli impianti di videosorveglianza ( se in essere) devono essere configurati in modo tale da ridurre al minimo l'utilizzazione dei dati personali e dei dati identificativi quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi.

### **10.5. Avvisi**

Gli interessati devono essere sempre informati che stanno per accedere o che si trovano in una zona/area videosorvegliata mediante apposizione di apposito cartello.

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli. L'avviso deve indicare il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia e dove reperire l'informativa estesa.

### **10.6. Tempi di conservazione delle immagini**

La conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

Ove il trattamento abbia finalità di vigilanza in assenza di eventi significativi la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici.

## **11. POLITICHE GENERALI RELATIVE ALLA COMUNICAZIONE DI DATI PERSONALI.**

La trasmissione di dati personali a terzi può avvenire:

- a) ove l'interessato abbia prestato il proprio consenso al trasferimento;



- b) ove sia necessario per adempiere ad un obbligo di legge ovvero la comunicazione dei dati risponda ad un rilevante interesse pubblico;
- c) ove vi sia legittimo interesse della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ prevalente rispetto a quello dell'interessato, ivi inclusi quelli:
  - i. della tutela del patrimonio, materiale e immateriale;
  - ii. della necessità di difesa della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ e del personale sanitario che opera alle sue dipendenze ovvero in base ad altra tipologia di contratto;
- d) ove vi sia un ordine dell'Autorità Giudiziaria competente.

La trasmissione di dati è sempre fatta in maniera non eccedente le prescrizioni stabilite dalle norme vincolanti che le dispongono e, ove ciò non contrasti con le stesse o con le finalità da esse perseguite, previa anonimizzazione dei dati.

I terzi destinatari devono essere stati nominati responsabili del trattamento, salvo ricorra a monte una ipotesi di contitolarità.

### **11.1. Politiche generali relative al trattamento dei dati del personale**

La presente politica generale riguarda la gestione dei dati personali relativa a tutti i lavoratori, intendendosi per tali tutte le persone che operano all'interno della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ per svolgere attività lavorativa. Sono considerati lavoratori ai fini della presente politica anche gli interessati che abbiano presentato domanda di assunzione o abbiano partecipato ad una procedura selettiva. Sono considerati lavoratori ai fini della presente politica anche quanti abbiano cessato la propria attività di collaborazione con la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ nella misura in cui i dati personali degli stessi rimangano nel possesso della società.

Il trattamento dei dati personali dei lavoratori ha la principale base giuridica nel contratto con il quale viene instaurato il rapporto di lavoro. Il contratto deve contenere in apposita clausola l'indicazione specifica dei trattamenti dei dati personali necessari all'esecuzione del rapporto di lavoro come risultanti dal Registro dei Trattamenti con la previsione che ulteriori trattamenti potranno rendersi necessari in conseguenza dello *ius variandi* della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ quale datore di lavoro.

Il medesimo contratto deve prevedere il diritto della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ di fondare il trattamento di dati personali del lavoratore:



- a) sulla necessità di adempiere ad un obbligo di legge o comunque previsto dal contratto collettivo tempo per tempo vigente;
- b) sulla necessità di tutelare un interesse legittimo del titolare con possibilità in questo caso del lavoratore di opporsi al trattamento per motivi preminenti rispetto a quelli del lavoratore;
- c) per la salvaguardia dell'interesse vitale del lavoratore con particolare riferimento ai trattamenti che riguardano la salute dei lavoratori;
- d) qualora il trattamento sia necessario per costituire, esercitare o difendere un diritto della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ per via giudiziaria.

In tutti i casi in cui non ricorra una delle sopra indicate ipotesi, all'atto di acquisire i dati personali deve essere richiesto il consenso del lavoratore con l'avvertenza che il rifiuto di prestarlo non ha nessuna conseguenza sul rapporto di lavoro né sulla sua prosecuzione. Ove i dati siano già in possesso della SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ il consenso è acquisito prima di iniziare il trattamento.

Il modulo del consenso sottoscritto dal lavoratore è inserito nel fascicolo personale di questo.

### **11.2. Comunicazione e diffusione di dati personali.**

I dati personali dei lavoratori sono coperti da segreto d'ufficio. il TITOLARE DEL TRATTAMENTO si assicura che ad essi abbiano accesso solo gli incaricati dello specifico trattamento per i quali sono raccolti.

I dati sono comunicati internamente per via adozione di sistemi di anonimizzazione e pseudonimizzazione ovvero in forma statistica e aggregata che non consenta di risalire alla posizione individuale del singolo salvo che

- a) la base giuridica del trattamento della funzione ricevente e la finalità del trattamento richiedano la trasmissione in forma nominativa;
- b) vi sia il consenso dell'interessato.

### **11.3. Dati sensibili dei lavoratori.**

I documenti, anche informatici, di qualunque genere contenenti dati personali dei lavoratori idonei a rivelarne

- a) l'origine razziale o etnica,
- b) le opinioni politiche;
- c) l'appartenenza sindacale;
- d) lo stato di salute;

devono essere conservati separatamente da ogni altro dato personale dell'interessato e comunque in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative e al fine di



impedire ogni accesso a tali dati da parte di soggetti non previamente designati come incaricati o responsabili del trattamento per il quale i dati sono raccolti.

### **12. DIRITTI DELL'INTERESSATO.**

Gli interessati, rispetto ai dati personali che li riguardano, hanno diritto di

- a) ottenere la conferma che sia in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e informazioni sui trattamenti;
- b) ottenere la rettifica dei dati personali inesatti che lo riguardano ovvero se pertinente rispetto al trattamento l'integrazione dei dati personali incompleti,
- c) ottenere la limitazione dei trattamenti;
- d) di ricevere copia elettronica dei dati personali che lo riguardano e da lui forniti;
- e) opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento automatizzato di dati.

### **13. VIOLAZIONE DEI DATI**

Gli incaricati del trattamento devono comunicare alla Presidenza di Mutua Nuova Sanità/titolare del trattamento e al *Data Protection Officer* la sottrazione di dati e di documenti non appena scoperti, senza ingiustificato ritardo, e comunque non oltre 72 ore dalla scoperta

La comunicazione deve indicare:

- a) la natura della violazione dei dati personali e le possibili cause;
- b) le categorie e il numero approssimativo di interessati e/o delle registrazioni dei dati personali in questione;
- c) le probabili conseguenze della violazione dei dati personali;
- d) e misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Ove dalla violazione possa sorgere pericolo per i diritti degli interessati. la SOCIETÀ DI MUTUO SOCCORSO MUTUA NUOVA SANITÀ provvede alla notificazione della violazione all'Autorità competente e agli interessati.