Manuale

Controllo delle copie	Distribuzione in forma controllata, copia n° ____
	Distribuzione in forma non controllata
AZIENDA	**Sanitaria Delfino Soc. Coop. Soc.**
SEDE	**Via Tivoli, 92015 Raffadali - AG**

Data revisione: 26/02/2025

INDICE

0. Introduzione

Il Manuale della Sicurezza è una misura minima di sicurezza per la protezione dei dati personali.
Alla **Sanitaria Delfino Soc. Coop. Soc.**, in qualità di Titolare del trattamento dei dati personali, competono le decisioni in ordine alle finalità ed alle modalità del trattamento degli stessi dati, compreso il profilo della sicurezza e della prevenzione da un potenziale Data Breach (violazione dei dati).
In considerazione di quanto sopra, gli obiettivi primari del presente Documento sono i seguenti:

- migliorare la consapevolezza dei rischi insiti nel trattamento dei dati con l'ausilio di strumenti elettronici, con particolare riferimento alla gestione e all'utilizzo del sistema informativo ed effettuare una valutazione di rischio sui trattamenti dei dati personali dell'Ente;
- individuare e definire adeguate misure tecniche ed organizzative finalizzate alla salvaguardia, alla corretta gestione e al corretto utilizzo del patrimonio informativo aziendale;
- adottare idonei presidi di controllo al fine di contenere i rischi, prevenendo le possibili situazioni di pericolo;
- fornire adeguate istruzioni comportamentali e procedurali ai soggetti coinvolti nella gestione dei singoli trattamenti.

Per il raggiungimento degli obiettivi imposti dal Regolamento (UE) 2016/679 e dal D.lgs.101/2018 la **Sanitaria Delfino Soc. Coop. Soc.** pone in essere, fra l'altro, le seguenti attività:

- censimento dei trattamenti effettuati e delle banche dati gestite dagli incaricati, al fine di individuare le diverse tipologie di dati trattati, i rischi potenziali e le conseguenti misure di sicurezza (art. 32 Reg.);
- predisposizione di un Documento di sintesi per il trattamento dei dati che raggruppa le regole deontologiche e le misure minime di sicurezza previste dal nuovo Regolamento (UE) 2016/679, in materia di protezione dei dati personali;
- predisposizione di una DPIA per l'individuazione delle misure atte a procedere alla valutazione del rischio normalizzate e valutazione del rischio intrinseco;
- predisposizione di appositi Registri delle attività del trattamento (art. 30 Reg.) dove verranno riportate tutte le informazioni relative a:

    - nome del titolare (o del responsabile del trattamento o del titolare per cui si agisce);
    - descrizione delle attività effettuate dal titolare (o per conto del titolare);
    - finalità del trattamento dei dati;
    - base giuridica del trattamento;
    - categorie di dati;
    - destinatari dei dati;
    - misure di sicurezza adottate;
    - termini per la cancellazione dei dati;
    - destinatati UE e Extra UE

1. Definizioni in materia di Privacy

Trattamento: qualsiasi operazione o insieme di operazioni compiute con o senza l'analisi di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, la conservazione, l'uso, la comunicazione mediante diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determinano le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi del trattamento di dati personali sono determinati dal diritto

dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dai paesi degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare del trattamento. Il Regolamento fissa in modo dettagliato le caratteristiche dell'atto con cui il Titolare del trattamento designa un Responsabile del trattamento, attraverso la stipula di un contratto o altro atto giuridico che regoli la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare.
Può essere nominato un responsabile interno mediante lettera di incarico.
Nei casi in cui vi siano servizi di outsourcing, l'outsourcer assume sempre la veste di Responsabile esterno e il trattamento dei dati da esso effettuato deve essere regolato da un contratto (anche il contratto di servizi stesso).
Incaricato: il dipendente che è coinvolto materialmente nel trattamento dei dati (ad es. amministrazione del personale) e incaricato attraverso un'apposita lettera di incarico.

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, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a una o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Es. Dati personali: codice fiscale e altri numeri di identificazione personale, nominativo, indirizzo o
altri elementi di identificazione personale, dati relativi alla famiglia e a situazioni personali, dati bancari o postali, carta identità, istruzione, formazione, dati relativi ai familiari, anche minori, del lavoratore iscritto.

Dati Particolari (ex sensibili): i 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 biomedici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Es. Dati particolari: adesione ad un sindacato, stato di salute, origine razziale ed etnica, convinzioni religiose filosofiche o di altro genere opinioni politiche, organizzazioni a carattere religioso, filosofico, politico o sindacale.

Responsabile della Protezione dei Dati (RDP ovvero DPO se si usa l'acronimo inglese Data Protection Officer): è un professionista con conoscenze specialistiche della normativa e della prassi designato dal titolare e/o dal responsabile del trattamento il quale garantisce standard di sicurezza adeguati. Può anche essere un dipendente del titolare o del responsabile del trattamento ovvero assolvere i suoi compiti in base a un contratto di servizi quale esterno. Il titolare o il responsabile del trattamento pubblica i dati di contatto del DPO e li comunica all'Autorità di controllo. Rientrano tra i suoi compiti la sensibilizzazione e la formazione del personale e la sorveglianza della valutazione d'impatto. In particolar modo: informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento o dalle altre disposizioni legislative
interne o europee in materia di protezione dati; sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento in tutte le sue parti, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento; fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento; cooperare con l'autorità di controllo fungendo, tra le altre cose, da punto di contatto per questioni connesse al trattamento effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.
è un soggetto indipendente che svolge un ruolo anche di mediatore nei rapporti tra gli interessati, i responsabili, il titolare e fa da tramite tra quest'ultimo e l'Autorità di controllo. Supporta tutti i soggetti che all'interno si occupano di privacy e hanno a che fare con il trattamento dei dati.

Modalità del Trattamento: il regolamento sancisce che il trattamento deve sempre ispirarsi ai principi di liceità, correttezza, trasparenza, pertinenza, compatibilità con le finalità espresse con gli scopi dichiarati, minimizzazione, proporzionalità, limitazione alla conservazione, sicurezza e integrità.

Data Breach (o violazione dei dati): tutti i titolari dovranno notificare all'autorità di controllo le violazioni dei dati personali di cui vengono a conoscenza entro le 72 ore e comunque senza "ingiustificato ritardo". La notifica dovrà avvenire solo se i titolari ritengano che dalla violazione derivino rischi per i diritti e le libertà dell'interessato. Nella logica del Regolamento, ispirato al principio della responsabilizzazione (accountability) di titolari e responsabili ovverosia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria in quanto è subordinata alla valutazione del rischio per gli interessati.
Tale valutazione spetta al titolare. E' altresì sancito che laddove la probabilità del rischio è elevata si dovrà informare della violazione anche l'interessato sempre "senza giustificato ritardo".

Liceità del Trattamento – Basi Giuridiche del Trattamento dei Dati
Il trattamento dei dati è lecito se ricorre almeno una delle seguenti condizioni:
- l'interessato ha prestato il consenso
- il trattamento è necessario all'esecuzione di un contratto
- il trattamento è necessario per adempiere ad un obbligo di legge
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico
- il trattamento è necessario per il perseguimento di un legittimo interesse del titolare

Consenso: come per la previgente normativa, il consenso deve essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto. Deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile". Il Regolamento prevede che il consenso deve essere esplicito per i dati particolari (ex sensibili) cosi come per il consenso basato su trattamenti automatizzati come ad esempio la profilazione. Il titolare deve essere sempre in grado di dimostrare che l'interessato ha prestato il proprio consenso a uno specifico trattamento. Per questo è richiesto che le informazioni e le comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Trova ingresso il principio che il
consenso dei minori è valido a partire dai 16 anni e prima di tale età il consenso è raccolto dai genitori o da chi ne fa le veci.

Informativa: il Regolamento, diversamente dal Codice, detta le caratteristiche dell'informativa in maniera più dettagliata nel senso che deve avere una forma coincisa, trasparente, intelligibile per l'interessato e facilmente accessibile. è necessario utilizzare un linguaggio chiaro e semplice e per i minori prevedere idonee informative. Generalmente l'informativa richiede la forma scritta e preferibilmente in formato elettronico ma sono ammessi anche altri mezzi, purché possa esserne data prova.

Contenuti dell'informativa: l'informativa deve:
- specificare i dati di contatto del Responsabile del trattamento e del RPD-DPO (ove esistente):
- indicare la base giuridica del trattamento;
- indicare qual è l'interesse legittimo del titolare;
- trasferimento dei dati personali in Paesi terzi e attraverso quali strumenti;
- periodo di conservazione dei dati;
- diritto di presentare ricorso all'autorità di controllo.

Tempi dell'informativa: se i dati non sono stati raccolti direttamente dall'interessato l'informativa deve essere fornita entro 1 mese dalla raccolta altrimenti al momento della comunicazione dei dati.

Diritti dell'interessato: il legislatore comunitario ha introdotto nuovi diritti in capo all'interessato:

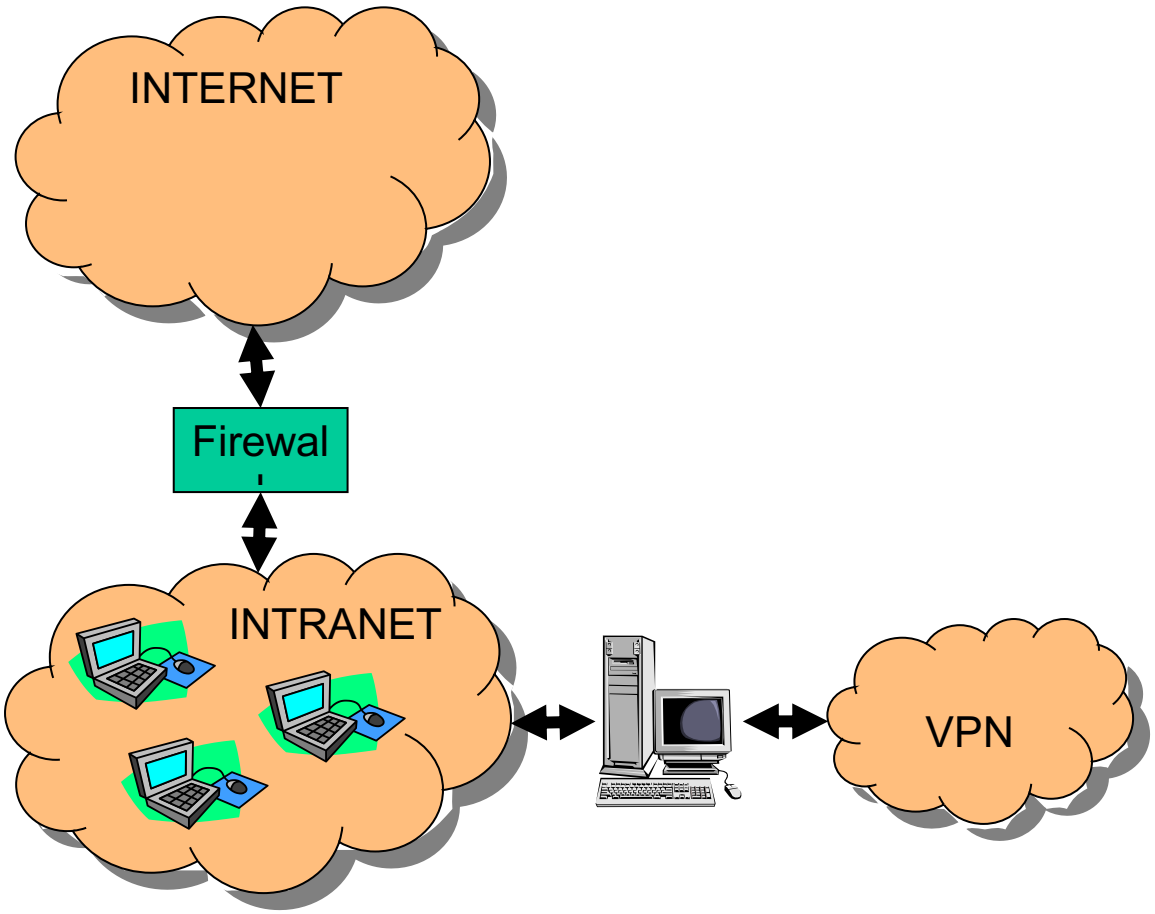
- diritto di accesso dell'interessato al trattamento dei propri dati;
- diritto di rettifica (senza ingiustificato ritardo);
- diritto all'oblio o diritto alla cancellazione dei dati;
- diritto di limitazione;
- diritto alla portabilità dei dati (da un titolare ad un altro);
- diritto di opposizione (al trattamento dei propri dati)

2. Architettura di sicurezza

In particolare dall'analisi delle funzionalità maggiormente a rischio e dall'analisi della localizzazione delle utenze e dei servizi si evince che:

1. la maggior parte delle utenze è collocata entro il confine aziendale e fruisce di servizi applicativi localizzati entro il confine aziendale;
2. esistono alcune utenze collocate fuori dal confine aziendale che accedono a funzionalità applicative gestite all'interno del confine – o comunque fornite da server che rientrano fra quelli di competenza dell'azienda -
    a. Tali utenti, utilizzano la rete telefonica pubblica commutata per eseguire gli accessi;

L'architettura che offre il miglior rapporto fra minimizzazione dei i rischi complessivi del sistema e costi di realizzazione e gestione è del tipo seguente:



L'architettura individuata si basa sul seguente criterio:

1. avere un confine organizzativo ben definito con pochi, e molto ben individuati, punti di attraversamento presidiati da dispositivi facilmente controllabili, gestibili e monitorabili.

3. Gestione e controllo profili di autorizzazione

3.1 Scopo
Lo scopo è quello di definire quali sono le modalità utilizzate per la gestione dei profili di autorizzazione, al fine di ottenere la conformità del servizio agli standard stabiliti.

3.2 Generalità
Il costante controllo e la corretta gestione dei profili di autorizzazione sono fondamentali ai fini della realizzazione ed erogazione di un servizio in grado di soddisfare pienamente le prescrizioni in materia di sicurezza del trattamento dei dati.
In relazione a quanto su esposto è indispensabile che tutto il Personale, in relazione alle mansioni svolte, osservi le disposizioni contenute nella presente procedura segnalando al Titolare e\o Responsabile Privacy ogni eventuale non conformità.

3.3 Campo di applicazione
La presente procedura di sistema si applica a tutti gli incaricati dell' Organizzazione che hanno accesso al sistema informativo, utilizzato per lo svolgimento delle attività attinenti alla realizzazione ed erogazione dei servizi.

3.4. Lista di distribuzione
La presente procedura viene inviata per la sua approvazione ed applicazione, in relazione alle specifiche competenze, a:

1. Titolare del trattamento dei dati

4.5 Procedura

- Per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, i profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
- Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
- Il Titolare provvede alla gestione e al controllo dei profili di autorizzazione.

LETTERE INCARICATI

4. Gestione Password

4.1 Scopo
Lo scopo è quello di definire quali sono le modalità utilizzate per la gestione delle credenziali di autenticazione, di definire le norme per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi, al fine di ottenere la conformità del servizio agli standard stabiliti.

4.2 Generalità
Il costante controllo e la corretta gestione delle credenziali di autenticazione sono fondamentali ai fini della realizzazione ed erogazione di un servizio in grado di soddisfare pienamente le prescrizioni in materia di sicurezza del trattamento dei dati.
In relazione a quanto su esposto è indispensabile che tutto il Personale, in relazione alle mansioni svolte, osservi le disposizioni contenute nella presente procedura segnalando al Titolare e\o Responsabile Privacy ogni eventuale non conformità.

4.3 Campo di applicazione
La presente procedura di sistema si applica a tutti gli apparati attivi che costituiscono il sistema informativo dell' Organizzazione, utilizzato per lo svolgimento delle attività attinenti alla realizzazione ed erogazione dei servizi.

ELENCO APPARATI ATTIVI DI RETE

4.4 Lista di distribuzione
La presente procedura viene inviata per la sua approvazione ed applicazione, in relazione alle specifiche competenze, a:

1. Titolare del trattamento dei dati

4.5 Procedura

1. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.
2. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
3. Tutti gli incaricati modificheranno al primo utilizzo e, successivamente, almeno ogni tre mesi la parola chiave assegnata dal titolare con una nuova composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito, e non contenente riferimenti agevolmente riconducibili all'incaricato.
4. Tutti gli incaricati consegneranno in busta chiusa le credenziali modificate al primo utilizzo e, successivamente, almeno ogni tre mesi al Titolare.
5. Il Titolare provvede alla custodia delle copie delle credenziali organizzando e garantendo la relativa segretezza.
6. Il Titolare provvede al monitoraggio delle credenziali di autenticazione.

GESTIONE DELLA PAROLA CHIAVE
GESTIONE CREDENZIALI DI AUTENTICAZIONE

5. Procedura di ripristino disponibilità dei dati

5.1 Scopo
Lo scopo è quello di definire quali sono i criteri e le modalità di ripristino della disponibilità dei dati nelle situazioni di malfunzionamento dei sistemi informatici al fine di evitare o minimizzare il disservizio arrecato agli utenti e garantire la disponibilità dei dati entro 7 giorni.

5.2 Generalità
Il caso più semplice di indisponibilità dei dati consiste nel deterioramento del supporto che contiene i dati, in genere un hard disk. Mentre tutto il resto delle apparecchiature(hardware e software), resta in perfetta efficienza. In questo caso le procedure di ripristino sono semplici e veloci (vedi step con *).
Se invece l' incidente dovesse coinvolgere l' intero locale dove risiedono i sistemi e i dati, verrà applicata la procedura in oggetto.

5.3 Campo di applicazione
La presente procedura di sistema si applica al Titolare del trattamento ed al responsabile della manutenzione dei sistemi informativi.

5.4 Lista di distribuzione
La presente procedura viene inviata per la sua approvazione ed applicazione, in relazione alle specifiche competenze, a:

2. Titolare del trattamento dei dati
3. Responsabile del sistema informativo

5.5 Procedura

- Attivare codice chiamata software house (*).
- Installazione hardware similare a quello non più disponibile.
- Installare lo stesso software di base e lo stesso software applicativo esistente sui sistemi non più agibili.
- Caricare i dati di back up (*).
- Aggiornamento dati (*)
- Configurare in rete il sistema.

RIPRISTINO DELLA DISPONIBILITA' DEI DATI
PROVA DI RIPRISTINO DATI

6. Elenco documenti GDPR

- ELENCO APPARATI ATTIVI DI RETE
- GESTIONE DELLA PAROLA CHIAVE
- GESTIONE CREDENZIALI DI AUTENTICAZIONE
- RIPRISTINO DELLA DISPONIBILITA' DEI DATI
- PROVA DI RIPRISTINO DATI
- ISTRUZIONI OPERATIVE INCARICATI TRATTAMENTO
- ISTRUZIONI OPERATIVE SISTEMI INFORMATICI
- ISTRUZIONI OPERATIVE DATA BREACH
- ISTRUZIONI OPERATIVE VIDEOSORVEGLIANZA
- ANAGRAFICA AZIENDA
- ORGANIGRAMMA
- DPIA
- REGISTRI
- INFORMATIVA FORNITORI
- INFORMATIVA DIPENDENTI
- INFORMATIVA CLIENTI
- NOMINA RESPONSABILE ESTERNO
- NOMINA MEDICO COMPETENTE
- NOMINA RESPONSABILE INTERNO
- NOMINA AMMINISTRATORE DI SISTEMA
- LETTERE INCARICATI

IL TITOLARE DEI TRATTAMENTI