

MODELLO ORGANIZZATIVO PRIVACY (MOP)

REGOLAMENTO UE 2016/679 (GDPR) E D. LGS N° 196 DEL
30/06/2003, MODIFICATO DAL D. LGS N° 101 DEL 10/08/2018

ALL.1 "GESTIONE DELL'ESERCIZIO DEI DIRITTI DELL'INTERESSATO"

ALL.2 "LINEE GUIDA PER LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

ALL. 3 "PROCEDURA PER LE VIOLAZIONI DI DATI PERSONALI" (DATA BREACH)

-

INDICE

1.	OBIETTIVI E DEFINIZIONI	pag.2
2.	GLOSSARIO	
3.	AMBITO DI APPLICAZIONE	pag. 3
4.	RISERVATEZZA DELLE INFORMAZIONI	pag. 4
5.	PRINCIPI GENERALI DEL TRATTAMENTO DATI	
6.	ATTUAZIONE DELLA POLICY	pag. 5
7.	IMPEGNO DEGLI ORGANI DI GOVERNO	
8.	SICUREZZA DELLE INFORMAZIONI	pag. 6
9.	ORGANIGRAMMA PRIVACY E REGISTRO DEI TRATTAMENTI- SISTEMA DI NOMINE E RESPONSABILITA'	pag. 7
	9.1 Titolare del Trattamento	pag. 8
	9.2 Il Responsabile della Protezione dei Dati o Data Protection Officer (DPO)	
	9.3 UFFICIO PRIVACY	pag.9
	9.4 DESIGNATI PRIVACY	pag.10
	9.5 AUTORIZZATI PRIVACY	pag. 12
	9.6 AMMINISTRATORE DI SISTEMA	pag. 13
10.	ACCESSO AI DATA BASE E PROFILI DI AUTORIZZAZIONE	pag. 14
11.	FORMAZIONE	
12.	TENUTA IN SICUREZZA DEI DOCUMENTI E DEGLI ARCHIVI	pag. 15
13.	INFORMATIVA ALL'UTENZA	
14.	DIRITTI DELL'INTERESSATO	pag. 16
15.	MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY	
16.	NORME COMPORTAMENTALI BASILARI PER I DIPENDENTI: il "clean desk & clear screen Policy"	
17.	ELENCO DOCUMENTAZIONE PRIVACY AZIENDALE	pag.18

1. OBIETTIVI E DEFINIZIONI

L'Azienda Socio Sanitaria Locale n. 7 del Sulcis Iglesiente (di seguito anche denominata "Asl") intende dotarsi di linee guida che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale.

Obiettivo del presente documento, e di quelli ad esso collegati, è definire il **Modello Organizzativo Privacy (Policy Privacy)**, ovvero individuare strategia, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla Asl, ai sensi del D. Lgs. 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*" (Codice Privacy), come modificato dal D. Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (*GDPR – General Data Protection Regulation*), nonché di ulteriori provvedimenti in materia in particolare quelli emessi dal Garante Europeo della Protezione dei Dati (GEPD) e dall'Autorità Garante Nazionale per la protezione dei dati personali.

2. GLOSSARIO

Ai fini del presente Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- Normativa: D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente Modello Organizzativo Privacy.
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*", come modificato dal Decreto Legislativo 10 agosto 2018, n. 101.
- Regolamento: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati).
- SGP: Sistema di Gestione della Privacy.
- 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 uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- 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.

- Interessato: la persona fisica cui si riferiscono i dati personali.
- Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- DPO: Data protection officer o Responsabile della protezione dei dati personali – il soggetto nominato dal Titolare ai sensi dell'art. 37 del Regolamento.
- Ufficio Privacy: la struttura aziendale preposta alla sorveglianza e al supporto in merito all'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento e, per quanto di sua competenza, dal DPO.
- Referente privacy (o designato): la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più o soggetti autorizzati al trattamento.
- Autorizzato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento.
- 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 del trattamento o del responsabile del trattamento.
- 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.
- Trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente inciderebbe in modo sostanziale sugli interessati in più di uno Stato membro.
- Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein).

3. AMBITO DI APPLICAZIONE

La **politica della privacy (policy)** che discende dal presente Modello Organizzativo Privacy si applica alla ASL nella sua interezza, a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.

Tutto il personale che, a qualsiasi titolo, collabora con la ASL ed è in qualche modo coinvolto con il

trattamento di dati e informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Privacy (SGP) è responsabile, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda devono garantire il rispetto dei requisiti contenuti nella politica della privacy (policy).

La politica della privacy (policy) della ASL deve essere inserita come parte integrante nella regolamentazione di qualsiasi accordo con tutti i soggetti esterni coinvolti con il trattamento di informazioni che rientrano nel campo del **Sistema di Gestione della Privacy (SGP)**.

4. RISERVATEZZA DELLE INFORMAZIONI

La ASL si impegna a garantire la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività in conformità alle procedure interne previste, coerenti con il presente Modello Organizzativo Privacy.

Il trattamento dei dati può essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste. Tutti i soggetti in qualsiasi modo coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione regolamentata eventualmente esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2105 del codice civile e dall'art. 12 del Codice di comportamento dei dipendenti pubblici.

La ASL si impegna a garantire adeguati livelli di sicurezza delle informazioni rese disponibili da terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

5. PRINCIPI GENERALI DEL TRATTAMENTO DATI

Il Titolare del trattamento si impegna a garantire e dimostrare che il trattamento dei dati personali avviene in maniera conforme a quanto previsto dalla normativa e che quindi siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati. A tal proposito sono state previste misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati nel "Regolamento per la gestione dell'esercizio dei diritti dell'interessato" All 1 al MOP;
- 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;
- 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.

Le presenti indicazioni sono valide, oltre che per i trattamenti dei dati personali di cui la ASL è Titolare, anche per tutti quei trattamenti per cui la ASL è nominata Responsabile del trattamento, salvo la presenza di misure più restrittive in materia di protezione dei dati personali contenute nei documenti che regolano i rapporti con il Titolare del trattamento.

Poiché analoghe garanzie di protezione e l'adozione di adeguate misure di sicurezza sono richieste ai soggetti terzi ai quali la ASL affida l'incarico di Responsabile del trattamento, la *policy* in oggetto è resa disponibile presso gli stessi.

6. ATTUAZIONE DELLA POLICY

Il Titolare del trattamento con il supporto del Responsabile della protezione dati, e per il tramite dell'Ufficio Privacy, deve:

- o condurre l'analisi dei rischi con le opportune metodologie e adottare le misure per la gestione del rischio;
- o stabilire le norme di comportamento necessarie alla conduzione sicura delle attività aziendali;
- o verificare le violazioni alla sicurezza, adottare le contromisure necessarie e controllare l'esposizione dell'Azienda alle principali minacce e rischi;
- o organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la qualità, l'integrità e la sicurezza delle informazioni;
- o verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Privacy (SGP).

Il personale della Asl che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno, potrà essere perseguito nelle opportune sedi, nel pieno rispetto dei vincoli di legge e contrattuali.

7. IMPEGNO DEGLI ORGANI DI GOVERNO

La Direzione della ASL sostiene attivamente le attività inerenti alla gestione della privacy, o protezione dei dati personali, tramite indirizzi precisi, impegno evidente, incarichi espliciti e riconoscimento delle responsabilità specifiche relative alla sicurezza delle informazioni.

L'impegno della Direzione si attua tramite un'adeguata struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi siano coerenti con la realtà della struttura a cui si riferiscono;
- stabilire i ruoli e relative responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione della Privacy (SGP);
- fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo,

revisione, gestione e miglioramento continuo del Sistema di Gestione della Privacy (SGP);

- controllare che il Sistema di Gestione della Privacy (SGP) sia integrato in tutti i processi aziendali e che le conseguenti procedure e controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni;
- attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

La ASL riconosce la propria responsabilità che discende dalla normativa vigente e si impegna a proteggere i dati personali che gli utenti affidano ad essa da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di tecnologie e procedure aziendali di protezione secondo le migliori pratiche (best practices) di volta in volta disponibili.

8. SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali la ASL assicura l'integrità e la protezione e consente l'accesso esclusivamente ai ruoli e alle funzioni necessarie, preventivamente autorizzate.

La mancanza di adeguati livelli di sicurezza può, infatti, comportare un danno di immagine alla Azienda, la mancata soddisfazione degli utenti, dei dipendenti degli stakeholder in genere, il rischio di incorrere in sanzioni legate alla violazione delle leggi vigenti nonché altri danni di natura economica e finanziaria.

Per conseguire sempre l'allineamento normativo e aumentare la capacità di controllo, la ASL ha istituito e mantiene aggiornato un Registro delle attività di trattamento.

La Asl identifica, quando ritenuto necessario a seguito delle risultanze dell'analisi dei rischi connessi al trattamento dei dati personali, le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che consente di acquisire un livello aggiuntivo di consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio, eseguita su tutti i trattamenti in essere o previsti, permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza al sistema informativo e in generale all'intera organizzazione, oltre a indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili presupposti, di seguito enunciati:

- Istituzione, con deliberazione del Direttore Generale n. 649 del 31/10/2023, di un Registro dei trattamenti dati personali, costantemente aggiornato, che riporta gli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno di essi è stato individuato, con deliberazione del Direttore Generale n. 124 del 21/02/2025, un Designato e gli "Autorizzati" al trattamento dei dati;
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;

- Gli accessi ai sistemi informativi sono sottoposti a una procedura di identificazione e autenticazione. Inoltre, le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e tali autorizzazioni sono periodicamente sottoposte a revisione;
- Sono indicate le misure di sicurezza per l'utilizzo sicuro dei dati (luoghi, mezzi di trasporto, strumenti) e delle informazioni aziendali in allegato al Registro dei trattamenti e oggetto di periodico aggiornamento;
- È incoraggiata la piena consapevolezza da parte del personale delle problematiche relative alla sicurezza delle informazioni;
- Per poter prevenire o almeno gestire in modo tempestivo gli incidenti, tutti sono chiamati a rendersi partecipi del sistema di sicurezza aziendale e pertanto devono notificare qualsiasi problema relativo alla sicurezza di cui sono a conoscenza;
- È necessario prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;
- È assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti;
- È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici;
- Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

9. ORGANIGRAMMA PRIVACY E REGISTRO DEI TRATTAMENTI- SISTEMA DI NOMINE E RESPONSABILITA'

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, la ASL garantisce sempre la precisa individuazione dei soggetti che ricoprono ruoli attivi nel trattamento. Ciò avviene con l'allestimento e il mantenimento efficiente nel tempo di un sistema tracciabile delle nomine e delle relative mansioni.

In questo modo risulta di immediata comprensione la conseguente ripartizione delle responsabilità di ogni soggetto, parametrata alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche analizzati ogni volta ritenuto necessario.

Quanto descritto trova riscontro nell'organigramma privacy che viene aggiornato a cadenza periodica ritenuta più opportuna in relazione al settore di attività e all'articolazione della propria organizzazione oppure in occasione di qualsiasi variazione intervenuta.

In accordo con la normativa di riferimento e con la policy che discende dal presente Modello Organizzativo Privacy, costituiscono figure imprescindibili quelle di seguito descritte.

9.1 Titolare del Trattamento

Il Titolare del trattamento è la Asl Sulcis Iglesiente nella persona del suo legale rappresentante in tale ruolo si impegna a:

- adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;
- nominare, con proprio atto, il Responsabile della Protezione dei Dati (DPO);
- adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare i Designati al trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai Designati al trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti Autorizzati al trattamento dei dati proposti dai Designati assumendo così un ruolo di effettivo controllo e indirizzo;
- assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

Inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire i loro diritti impegnandosi a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

9.2 Il Responsabile della Protezione dei Dati o Data Protection Officer (DPO)

Il Responsabile della Protezione dei Dati o Data Protection Officer (DPO), previsto obbligatoriamente dal Regolamento UE 2016/679 artt. 37,38 e 39, è nominato con atto formale del Direttore Generale.

Il DPO deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare sulla base di un contratto di servizio o essere un dipendente dell'azienda, in tal caso deve svolgere il suo ruolo in modo indipendente senza nessun vincolo o subalternità.

L'ASL mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati trattati.

Il DPO svolge i seguenti compiti:

- a) informa e fornisce consulenze al Titolare del Trattamento, nonché ai Designati ed Autorizzati (dipendenti) che eseguono il trattamento dei dati in merito agli obblighi;
- b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del Trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- c) fornisce pareri, qualora vengano richiesti, in merito alla valutazione d'impatto sulla protezione dei dati e sorveglianza i relativi adempimenti;
- d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva, di cui al presente Regolamento;
- f) assiste il Titolare ed i Designati, nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati, per quanto riguarda gli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
- g) fornisce parere al Titolare del Trattamento per la predisposizione e per la definizione del Registro delle attività di trattamento, in collaborazione con l'Amministratore di Sistema e con le altre strutture competenti dell'ASL, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
- h) verifica l'approntamento e l'erogazione dell'informativa afferente il trattamento dei dati personali presso l'Azienda;
- i) vigila sull'osservanza del presente regolamento e fornisce consulenza ai dipendenti sulle problematiche riguardanti la normativa in materia di protezione dei dati personali;
- l) vigila sulla costituzione e l'aggiornamento dei seguenti archivi:
- Elenco dei Designati, Autorizzati, dei Responsabili dei Trattamenti, con i relativi recapiti;
 - Elenco delle banche dati afferenti i dati personali custoditi dall'ASL;
- m) valuta la documentazione privacy implementata dal Titolare del Trattamento ovvero dai Designati ai fini dell'applicazione della normativa vigente e del presente regolamento;
- n) propone interventi di formazione a livello aziendale, in tema di normativa sulla protezione dei dati personali.

9.3 UFFICIO PRIVACY

Alla luce dell'analisi dei rischi aziendali in materia di trattamento dei dati personali, il Titolare ha ritenuto opportuno procedere alla identificazione dell'Ufficio Privacy, organizzato all'interno della SC Affari Generali e Legali. Il Referente dell'Ufficio Privacy è individuato tra i collaboratori amministrativi con formazione in discipline giuridiche ed esperienza consolidata nel settore. La sua nomina è disposta su proposta del Responsabile della SC Affari Generali e legali le sue attività sono esercitate in virtù della delega conferita dal Titolare del Trattamento, che le attribuisce per il tramite del Responsabile della SC Affari Generali e Legali garantendo così un'applicazione uniforme delle disposizioni normative e il corretto funzionamento

Di seguito si riportano le funzioni qualificanti principali:

- supporta la Direzione Aziendale impostando le procedure per la corretta applicazione della normativa di settore e ne cura gli adempimenti;
- vigila sull'effettivo funzionamento delle prescrizioni adottate dalla Direzione Aziendale in materia di protezione dei dati personali;
- supporta il Responsabile della Protezione dei Dati nella valutazione della necessità di effettuare una valutazione d'Impatto sulla Protezione dei Dati (DPIA) e collabora alla sua redazione, in conformità all'art.35 del GDPR
- conserva e aggiorna l'elenco dei Designati e degli Autorizzati al trattamento dei dati personali;
- adempie ai pareri, agli indirizzi e alle raccomandazioni del Responsabile della Protezione dei Dati (DPO) per la conformità della Asl al Regolamento (UE) 2016/679;
- predispone adeguati flussi di comunicazione da e verso il Responsabile della Protezione dei Dati (DPO), ivi inclusi gli allarmi (alert) e le violazioni (data breach) di sistema;
- fornisce al Responsabile della Protezione dei Dati (DPO) accesso alle informazioni necessarie per lo svolgimento dei compiti a quest'ultimo attribuiti;
- svolge un compito di collegamento tra i Designati e gli Autorizzati al trattamento dei dati personali e il Responsabile della Protezione dei Dati (DPO);
- gestisce operativamente il Registro dei trattamenti del Titolare del trattamento;
- coinvolge il Responsabile della Protezione dei Dati (DPO) in questioni di particolare complessità;
- informa tempestivamente il Titolare del trattamento in caso di violazione dei dati personali (data breach) e fornisce aggiornamenti fino alla risoluzione dell'incidente;

9.4 DESIGNATI PRIVACY

I soggetti Designati per la privacy sono nominati dal Titolare del trattamento presso le Unità Organizzative da loro dirette e in cui vengono svolti i trattamenti dei dati personali relative alla loro competenza.

I compiti del soggetto Designato privacy, con apposito atto, sono di seguito sintetizzati:

- **con riferimento al personale assegnato**

1. individuare e nominare per iscritto i soggetti autorizzati al trattamento dei dati personali, identificati nelle persone che operano nella Struttura assegnata, secondo le rispettive competenze, provvedendo ad aggiornare l'elenco degli stessi a seconda di nuovi ingressi di personale o di variazione dell'assegnazione delle competenze;
2. fornire agli autorizzati specifiche istruzioni operative riguardanti le operazioni di raccolta, trattamento e archiviazione dei dati personali su supporto informatico e cartaceo, individuando puntualmente l'ambito di trattamento consentito;
3. vigilare sul rispetto delle istruzioni impartite agli autorizzati e garantire che il trattamento dei dati avvenga

in modo lecito e corretto, nel rispetto dei principi di cui all'art. 5 del Regolamento europeo sulla protezione dei dati n. 2016/679 (d'ora in avanti GDPR) quindi:

- che i dati siano raccolti per finalità determinate, esplicite e legittime (limitazione della finalità);
 - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
 - esatti e, se necessario, aggiornati (esattezza),
 - conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);
 - trattati in maniera da garantire un'adeguata sicurezza, 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);
4. vigilare sul rispetto delle misure di sicurezza da parte del personale autorizzato, al fine di evitare rischi, anche accidentali, di distruzione o perdita di dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del trattamento;
5. garantire la partecipazione del personale autorizzato agli eventi formativi organizzati dall'Azienda in materia di protezione dei dati;
6. garantire che i profili di accesso ai sistemi informativi da parte delle persone AUTORIZZATE al trattamento dei dati personali siano configurati anteriormente all'inizio del trattamento, nonché verificare, periodicamente, secondo le procedure aziendali, che tali profili siano conformi con le mansioni svolte. In caso di sospensione dall'attività lavorativa o revoca/esclusione dall'incarico dovrà essere comunicato alle strutture competenti la necessità di procedere alla disattivazione dell'utenza;
7. attenersi scrupolosamente alle disposizioni previste dal GDPR e alle procedure e istruzioni emanate in materia di privacy dal Titolare del trattamento;
8. comunicare al Titolare e al DPO (agli indirizzi e-mail direzione.generale@aslsulcis.it e dpo@aslsulcis.it) eventuali nuovi trattamenti ovvero le modifiche relative alle attività di trattamento in corso - anche nel caso di passaggio dalla modalità cartacea a quella elettronica - nonché gli eventuali mutamenti tecnici che possano incidere direttamente sui medesimi;
9. collaborare per il censimento dei trattamenti al fine dell'aggiornamento del Registro dei trattamenti;
10. assicurare che i dati da pubblicare sul sito istituzionale, siano conformi alla normativa in materia e siano rispettati gli obblighi di trasparenza e tracciabilità, come previsto dal Codice di Comportamento aziendale;
11. distruggere i dati personali in caso di cessazione del trattamento provvedendo alle formalità di legge;
12. designare una persona di riferimento (Referente Privacy di Struttura) che avrà il compito di mantenere i contatti e collaborare con il Titolare, l'Ufficio Privacy e il DPO.

- **con riferimento alle misure di sicurezza**

13. informare tempestivamente il Titolare e il DPO su qualsiasi evento che possa compromettere il corretto

trattamento e la sicurezza dei dati (anomalie, furti, perdite accidentali o distruzioni dei dati) al fine di attivare, nel caso sia riscontrato un rischio per i diritti e le libertà delle persone fisiche, la procedura aziendale del Data Breach;

14. adottare e rispettare le misure di sicurezza tecniche e organizzative previste dalla normativa vigente e dai provvedimenti del Garante, nonché eventuali misure ritenute idonee individuate dal Titolare, atte a preservare la disponibilità e integrità del dato;

15. custodire e conservare i supporti utilizzati per le copie dei dati;

16. verificare periodicamente le modalità di accesso ai locali e le misure adottate per la loro protezione;

17. comunicare le Misure di sicurezza adottate al SC Affari Generali e Legali (ufficio.privacy@aslsulcis.it) al fine dell'aggiornamento del Registro dei Trattamenti;

- **con riferimento all'utenza:**

18. provvedere a che vengano fornite le informazioni di cui agli articoli 13 e 14 del GDPR ai soggetti interessati ogniqualvolta si raccolgano dati personali. Sorvegliare che siano affissi i cartelli contenenti le informazioni di cui sopra in tutti i luoghi in cui vengono erogate prestazioni (sanitarie, di prevenzione, amministrative socio-sanitarie, ecc. ...);

19. integrare le informazioni da rendere ai soggetti interessati e i moduli di consenso per i trattamenti per cui tale base legale sia necessaria, sentiti il Titolare e il DPO;

20. predisporre le soluzioni organizzative necessarie a garantire e agevolare l'effettivo esercizio del diritto d'accesso, senza ledere il diritto alla privacy dell'interessato;

21. segnalare all'Ufficio Privacy eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;

Il Designato deve altresì provvedere all'espletamento di tutte le operazioni necessarie per il rispetto e la corretta applicazione della normativa europea e nazionale vigente in materia di Privacy, collaborare con il Titolare nell'espletamento dell'attività di valutazione di impatto, ai sensi dell'art. 35 del GDPR e partecipare direttamente alle iniziative formative organizzate dall'Azienda sul tema della protezione dei dati. Il Designato, nell'ambito dei suoi poteri gestionali e di controllo, è tenuto a comunicare tempestivamente al Titolare, al DPO e all'Ufficio Privacy e i soggetti incaricati di eventuali ispezioni.

9.5 AUTORIZZATI PRIVACY

Il Designato privacy nomina, presso la propria Unità Organizzativa in cui vengono svolti i trattamenti, i soggetti Autorizzati al trattamento dei dati (o Autorizzati Privacy)

Il soggetto autorizzato effettua tutte le operazioni di trattamento dei dati personali attinenti all'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Titolare (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso.

In particolare, i compiti a esso attribuiti sono così sintetizzati:

- segnalare all'Ufficio Privacy nel caso di dipendenza diretta, eventuali richieste ricevute da parte

dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;

- avvisare il Referente privacy da cui dipende, o l'Ufficio Privacy nel caso di dipendenza diretta, se nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei principi di privacy by design e privacy by default;
- informare immediatamente l'Ufficio Privacy nel caso di dipendenza diretta, qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dei dati;
- segnalare all'Ufficio Privacy nel caso di dipendenza diretta, eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento).

9.7 AMMINISTRATORE DI SISTEMA

E' la figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (system administrator), ovvero una base dati (database administrator), ovvero reti e apparati di telecomunicazione di sicurezza (network administrator) è nominata persona autorizzata al trattamento dei dati personali.

Secondo quanto previsto dal Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)", l'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

Pertanto, la nomina ad Amministratore di Sistema deve essere individuale, esplicitata in forma scritta, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.

L'Amministratore di sistema ha le seguenti responsabilità:

- sovrintende alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con l'Ufficio Privacy, nello specifico ambito di operatività, fornisce guida e supporto ai Referenti Privacy e ai soggetti autorizzati in merito al trattamento dei dati personali;
- amministra e gestisce la sicurezza informatica operando anche come gestore e custode delle password;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, in merito a quanto previsto dal Regolamento sull'utilizzo degli strumenti aziendali informatici del Sistema di Gestione della Privacy (SGP);
- individuare i soggetti a cui affidare l'incarico di manutentore del sistema stesso.

Per consentire all'Amministratore di Sistema di svolgere adeguatamente le proprie funzioni, allo stesso

vengono concesse dal Titolare del trattamento le “Autorità di sistema”, che consistono nell’assegnazione di attributi, privilegi, o accessi che consentono la gestione delle “risorse critiche del sistema operativo”, ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

L’elenco dei soggetti nominati Amministratori di Sistema è conservato adeguatamente e consegnato in copia per la custodia all’Ufficio Privacy.

10. ACCESSO AI DATA BASE E PROFILI DI AUTORIZZAZIONE

Nel rispetto del principio di minimizzazione e limitazione della finalità del trattamento dei dati personali, i profili di accesso ai gestionali informatici aziendali sono configurati sulla base delle attività affidate a ciascun autorizzato e nel rispetto degli ambiti di trattamento consentiti.

L’assegnazione dei predetti profili ai singoli operatori incaricati del trattamento dei dati è effettuata a cura dei rispettivi responsabili del trattamento con abilitazioni calibrate alle rispettive mansioni operative.

Il trattamento dei dati deve, pertanto, essere evitato ogni volta in cui lo stesso non sia indispensabile per il perseguimento degli scopi prefissati.

Periodicamente i Designati del trattamento dati aggiornano i profili di autorizzazione del personale assegnato.

Tutti i dispositivi della ASL concessi in dotazione ai dipendenti vengono formattati a seguito delle

dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti della ASL sono, pertanto, tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne affinché venga assicurata la continuità dei servizi erogati e la conservazione dei documenti di lavoro.

Al fine di garantire che il trattamento dei dati inerenti allo stato di salute degli interessati sia effettuato con un idoneo livello di sicurezza, gli accessi ai software contenenti dati particolari devono essere tracciati.

11. FORMAZIONE

L’obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dalla ASL anche e soprattutto grazie alla particolare attenzione riposta nei confronti della formazione del proprio personale.

A tale scopo il Modello Organizzativo Privacy è divulgato presso il personale già in servizio e, nel caso di nuove risorse umane inserite in organico, fin dal momento del loro ingresso nella compagine della ASL. Per gli stessi fini di conoscenza, eventuali aggiornamenti sono diffusi con gli strumenti ritenuti di volta in volta più efficaci.

Allo scopo di creare un ecosistema favorevole nell’ambiente di lavoro e formare con particolare cura i soggetti che, per il ruolo ricoperto, risultano inseriti nel Sistema di Gestione della Privacy (SGP), la ASL:

- adotta un piano formativo annuale con l'obiettivo di alfabetizzazione iniziale in materia di protezione dei dati personali, destinato a tutto il personale della Asl;
- prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutti i dipendenti della società;
- conserva la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

La formazione dei soggetti autorizzati al trattamento e, ove ritenuto necessario, delle altre figure chiave nel Sistema di Gestione della Privacy (SGP), riguarda in particolare:

- gli aspetti generali della disciplina di protezione dei dati personali;
- le minacce, le vulnerabilità, la probabilità di accadimento e di conseguenza i rischi che minacciano i dati trattati;
- le conseguenze derivanti dalla violazione dei dati personali (Data Breach);
- le procedure da seguire in caso di violazione dei dati personali;
- le misure di prevenzione per evitare o almeno ridurre la probabilità di accadimento delle violazioni e le misure di mitigazione del danno in caso si verifichino;
- l'addestramento specifico per aggiornare il personale sulle misure di sicurezza e protezione dei dati personali ritenute adeguate e adottate dal Titolare del trattamento.

12. TENUTA IN SICUREZZA DEI DOCUMENTI E DEGLI ARCHIVI

Gli archivi che custodiscono i dati di cui l'Azienda è Titolare del trattamento, sia cartacei che digitali, devono essere collocati in locali non esposti a rischi ambientali in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo aziendale.

La documentazione archiviata, anche digitalmente, che riporta dati personali è conservata soltanto per il tempo previsto dalla legge e poi sottoposta a scarto di archivio o cancellata definitivamente.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Responsabile del trattamento dei dati di competenza oltre che dal Responsabile della gestione documentale che deve assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.

Per quanto riguarda la documentazione cartacea facente parte dell'archivio aziendale storico e/o di deposito, l'Azienda predispone periodicamente un piano di scarto d'archivio

13. INFORMATIVA ALL'UTENZA

L'Azienda fornisce un'informativa di carattere generale a tutti gli utenti/pazienti relativa alle modalità dei trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie.

L'Azienda predispone altresì informative specifiche sul trattamento dei dati personali relativi a particolari pazienti/utenti effettivamente interessati.

Le informative sono fornite per iscritto o con mezzi elettronici e riportano in modo chiaro e comprensibile, in forma concisa e trasparente tutte le informazioni relative alle modalità e finalità del trattamento dei dati personali e quali sono i diritti degli interessati.

14. DIRITTI DELL'INTERESSATO

Gli interessati possono contattare l'Ufficio Privacy o il Responsabile per la protezione dati (alias DPO) per tutte le questioni relative al trattamento dei propri dati personali e per l'esercizio dei propri diritti elencati negli artt. dal 15 al 22 (diritto di accesso ai dati; diritto di rettifica; diritto alla cancellazione; diritto di limitazione del trattamento; diritto alla portabilità; diritto di opposizione, diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato compresa la profilazione).

Il Sistema Gestione della Privacy comprende le procedure per la gestione delle richieste degli interessati finalizzate all'esercizio dei diritti sopra elencati con individuazione delle figure coinvolte e delle tempistiche da osservare.

Per la gestione dell'esercizio dei diritti dell'interessato si rimanda all'allegato 1 del presente MOP.

15. MONITORAGGIO DEL SISTEMA GESTIONE PRIVACY

La Direzione aziendale verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema di Gestione della Privacy (SGP), in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

L'Ufficio Privacy ha il compito di condurre operativamente la revisione di questa politica. Questi dovrà utilizzare opportuna modulistica, predisposta in modo da garantire omogeneità del confronto e facilitare il controllo dei risultati nel corso del tempo. I risultati della revisione periodica sono da sottoporre ai livelli decisionali superiori per le opportune deliberazioni.

La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate.

Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy (SGP).

16. NORME COMPORTAMENTALI BASILARI PER I DIPENDENTI: il "clean desk & clear screen Policy"

La politica della **scrivania sgombra** (*Clean Desk Policy*) e dello **schermo inattivo** (*Clear Screen Policy*) è una delle migliori strategie da attuare per ridurre il rischio di violazioni della sicurezza della postazione di lavoro.

Lo scopo di tale politica è stabilire requisiti minimi per prevenire violazioni accidentali o dolose dei dati personali (*Data Breach*) e responsabilizzare i soggetti che nelle attività lavorative si trovano a loro contatto.

Di seguito sono elencati i comportamenti virtuosi da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati sensibili e/o alle categorie particolari di dati personali non devono essere lasciate su una scrivania non presidiata;
- i laptop devono essere bloccati con un cavo di bloccaggio o conservati in un cassetto se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra, sotto o nei pressi di un computer, né possono essere lasciate per iscritto in posizione accessibile;
- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggidocumenti appositi;
- le lavagne contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere cancellate;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere conservati in cassette chiuse a chiave.

Per quanto non espressamente previsto dalla presente disposizione si rimanda a quanto previsto dal Codice di comportamento dei Pubblici dipendenti approvato con DPR 16 aprile 2013, n. 62 così come aggiornato dal DPR 81/2023, e alle disposizioni degli art 11 e 12 del Codice di comportamento aziendale approvato con delibera del Direttore Generale della Asl Sulcis Iglesiente n. 669 del 30/08/2024 (link <https://www.aslsulcis.it/amministrazione-trasparente/disposizioni-general/atti-general/codice-di-comportamento/>)

Il dipendente che viola queste norme di comportamento è soggetto alle azioni disciplinari previste, fino al licenziamento.

17. ELENCO DOCUMENTAZIONE PRIVACY AZIENDALE

Il sistema privacy aziendale della Asl Sulcis Iglesiente è composto dalla seguente documentazione di cui quella allegata è oggetto di adozione insieme al presente atto:

a. Modello organizzativo privacy:

- Procedure di distribuzione delle funzioni in materia di protezione dei dati (Nomine);
- Mappatura dei trattamenti (Registro delle attività di trattamento);
- Istruzioni formali alle persone autorizzate al trattamento sotto l'autorità del titolare (Nomine ad autorizzate al trattamento);
- Modulistica per le Informative ed eventuali modelli di richiesta Consenso;
- Contratti con responsabili del trattamento ed eventuali sub-responsabili (schema di atto di nomina).

b. Metodologia di valutazione d'impatto sulla protezione dei dati e procedura DPIA;

c. Procedura per la gestione dei diritti dell'interessato (artt. 15 a 22);

d. Relazione annuale del responsabile della protezione dei dati (RPD);

e. Procedure di gestione dei data breach e relativo registro.

Il Sistema di gestione della Privacy comprende anche la formazione annuale dei dipendenti ASL Sulcis Iglesiente, da pianificare con apposito atto entro il 15 gennaio di ogni anno in collaborazione con la formazione Ares Sardegna.