

SERVIZIO SANITARIO  
REGIONE AUTONOMA DELLA SARDEGNA  
**AZIENDA SANITARIA LOCALE N. 2**  
**Olbia**

DELIBERAZIONE DEL COMMISSARIO N. 40 DEL 11/10/2010

**OGGETTO: LINEE DI INDIRIZZO E DI PROGRAMMAZIONE IN MATERIA DI TRATTAMENTO  
DATI - INDIVIDUAZIONE DEI RESPONSABILI DEL TRATTAMENTO E  
ADOZIONE DI SCHEMI TIPO DI PROVVEDIMENTI DI INCARICO**

L'anno duemiladieci il giorno undici del mese di gennaio in Olbia,  
nella sede legale dell'Azienda Sanitaria Locale n. 2.

**IL COMMISSARIO**

**Dottor GIOVANNI ANTONIO FADDA**

Sentiti i pareri favorevoli del

DIRETTORE AMMINISTRATIVO

Avv. Mario Giovanni Altana

e del

DIRETTORE SANITARIO

Dott.ssa Maria Serena Fenu

**PREMESSO** quanto segue:

- ai sensi ed in attuazione delle disposizioni contenute nel Dlgs 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali", in qualità di "Titolare" (art. 28 Dlgs 196/2003) del trattamento dati, è necessario: a) adottare linee di indirizzo e di programmazione in materia di trattamento dei dati personali, sensibili e giudiziari;
- b) individuare i "Responsabili" del trattamento (art. 29 Dlgs 196/2003); c) adottare schemi tipo di provvedimenti di incarico di responsabile e di "Incaricato" del trattamento (art. 30 Dlgs 196/2003);
- i responsabili del trattamento sono stati individuati alla luce del nuovo assetto organizzativo delineato con l'atto aziendale ed in correlazione con l'attribuzione delle responsabilità delle strutture del più alto livello gestionale; l'incarico di responsabile è indissolubilmente connesso con l'attribuzione dell'incarico dirigenziale di riferimento;
- l'Area Affari Generali, Legali e Comunicazione ha predisposto le unite linee di indirizzo e di programmazione in materia di trattamento dei dati personali, sensibili e giudiziari e relativi allegati, che sono condivisi;

**Visti:** il D. Lgs. 30 dicembre 1992 n. 502 e successive modificazioni ed integrazioni;  
la L.R. 24 marzo 1997, n. 10;  
la L.R. 28 luglio 2006, n. 10;  
il Dlgs n. 196/2003;

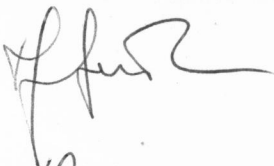
### **DELIBERA**

Per le motivazioni espone in premessa e qui integralmente richiamate:

- 1) di approvare le linee di indirizzo e di programmazione e relativi allegati di cui al documento unito alla presente che è parte integrante e sostanziale del presente provvedimento;
- 2) di dare atto che il presente provvedimento è necessario per procedere, in qualità di "Titolare" (art. 28 Dlgs 196/2003) del trattamento dati ed alla luce del nuovo assetto organizzativo delineato con l'atto aziendale, all'esatta individuazione delle aree di responsabilità connesse rispettivamente alle figure di "Responsabile" (art. 29 Dlgs 196/2003) e di "Incaricato" (art. 30 Dlgs 196/2003) del trattamento dei dati, rinviando a successivi provvedimenti la formalizzazione delle designazioni in capo ai singoli soggetti coinvolti nel trattamento dei dati personali, in base agli schemi tipo approvati;
- 3) di trasmettere la presente deliberazione a tutti i Direttori di struttura aziendale.
- 4) di incaricare l'Area Affari Generali, Legali e Comunicazione della formalizzazione degli incarichi di Responsabile del trattamento dati e di dare incarico al Servizio Amministrazione del Personale di informare tempestivamente il Referente Aziendale per la Privacy di ogni modificazione relativa agli incarichi di Direttore delle strutture aziendali.

**IL DIRETTORE SANITARIO**

(Dott.ssa Maria Serena Fenu)

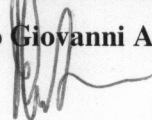


RDG



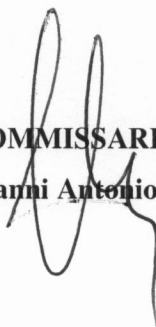
**IL DIRETTORE AMMINISTRATIVO**

(Avv. Mario Giovanni Altana)



**IL COMMISSARIO**

(Dott. Giovanni Antonio Fadda)



da compilarsi a cura del Servizio / Struttura proponente/estensore

(luogo e data) \_\_\_\_\_, \_\_\_\_/\_\_\_\_/\_\_\_\_.

La presente deliberazione:

... è soggetta al controllo ai sensi dell'art. 29, comma 1, lettere a), b), c), della Legge Regionale 28.7.2006 n. 10.

oppure

... deve essere comunicata al competente Assessorato regionale ai sensi dell'articolo 29, comma 2, della Legge Regionale 28.7.2006 n. 10

Il Responsabile del Servizio/Struttura \_\_\_\_\_ (proponente/estensore)

(firma) \_\_\_\_\_

Si certifica che la presente deliberazione è pubblicata all'Albo Pretorio dell'Azienda Sanitaria Locale n. 2 di Olbia

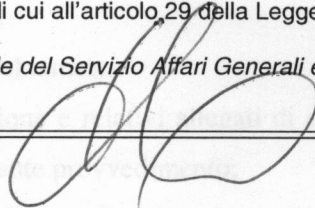
dal 08/01/2010, e che:

è esecutiva dal giorno della pubblicazione ai sensi della Legge Regionale 28.7.2006 n. 10.

... con lettera in data \_\_\_\_/\_\_\_\_/\_\_\_\_, protocollo n. \_\_\_\_\_, è stata inviata all'Assessorato Regionale dell'Igiene, Sanità e Assistenza Sociale per il controllo di cui all'articolo 29 della Legge Regionale 28.7.2006 n. 10.

Olbia, 08/01/2010.

Il Responsabile del Servizio Affari Generali e Legali



La presente deliberazione:

... è divenuta esecutiva, ai sensi dell'articolo 29 della Legge Regionale 28.7.2006 n. 10, in virtù della Determinazione del Direttore del Servizio \_\_\_\_\_ dell'Assessorato Regionale dell'Igiene, Sanità e Assistenza Sociale n. \_\_\_\_\_ del \_\_\_\_/\_\_\_\_/\_\_\_\_.

... è stata annullata, ai sensi dell'articolo 29 della Legge Regionale 28.7.2006 n. 10, in virtù della Determinazione del Direttore del Servizio \_\_\_\_\_ dell'Assessorato Regionale dell'Igiene, Sanità e Assistenza Sociale n. \_\_\_\_\_ del \_\_\_\_/\_\_\_\_/\_\_\_\_.

... è divenuta esecutiva per decorrenza dei termini per il controllo, ai sensi dell'articolo 29 della Legge Regionale 28.7.2006 n. 10.

Olbia, \_\_\_\_/\_\_\_\_/\_\_\_\_.

Il Responsabile del Servizio Affari Generali e Legali

Per copia conforme all'originale esistente agli atti della Azienda Sanitaria Locale n. 2, per uso

Olbia, \_\_\_\_/\_\_\_\_/\_\_\_\_.

Il Responsabile del Servizio Affari Generali e Legali

## Allegato

### Linee di indirizzo e di programmazione in attuazione del Dlgs 30.06.2003 n. 196

#### “Codice in materia di protezione dei dati personali”

##### PRINCIPI FONDAMENTALI

L'Azienda Sanitaria Locale n. 2 di Olbia, nell'ambito della propria organizzazione e dell'attuazione dei fini istituzionali, garantisce, ai sensi dell'art. 2 del Dlgs n. 196/03, che il trattamento dei dati personali, sensibili, giudiziari si svolga nel pieno rispetto della tutela dei diritti, delle libertà fondamentali e della dignità dell'interessato, con particolare attenzione alla riservatezza, all'identità personale ed al diritto alla protezione dei dati stessi.

Il trattamento dei dati deve sempre essere improntato ai sei principi di semplificazione, armonizzazione, efficacia, correttezza, liceità, legittimità, indispensabilità e non eccedenza rispetto agli scopi per i quali sono raccolti i dati stessi.

##### TITOLARE DEL TRATTAMENTO

In base al combinato disposto degli artt. 4, comma 1, lett f) e 28 del Dlgs n. 196/2003, il "titolare del trattamento", con riferimento alla Pubblica Amministrazione, è l'entità nel suo complesso alla quale competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. In attuazione delle disposizioni di cui sopra, **il titolare del trattamento è, pertanto, l'Azienda Sanitaria Locale n. 2 di Olbia intesa quale entità oggettivamente considerata, nella persona del suo legale rappresentante.**

##### DEFINIZIONE DEI LIVELLI DI RESPONSABILITÀ

Sulla base di quanto sopra premesso, al fine di garantire la corretta ed effettiva applicazione delle disposizioni di legge, si rende opportuno, in ambito aziendale:

- individuare i necessari profili di responsabilità collegati agli adempimenti previsti dalla normativa vigente; a tale scopo al presente atto di indirizzo è **allegato sub 1 l'elenco delle strutture i cui Direttori debbono essere nominati responsabili del trattamento**, con riferimento ai singoli ambiti di competenza, cui saranno attribuiti gli incarichi formali come da **schema tipo di provvedimento allegato sub 2**; l'elenco dei responsabili sarà di volta in volta aggiornato in seguito a nuove nomine e/o ad avvicendamenti degli incarichi a cura del referente aziendale per la privacy; ove l'incarico di struttura non sia attribuito sarà

nominato responsabile delle relative banche dati il responsabile di struttura complessa nella quale la struttura semplice è inserita o il responsabile di dipartimento.

- nell'esercizio dei poteri di indirizzo, di individuazione degli obiettivi, di definizione dei profili organizzativi nonché di adozione di direttive generali in materia di trattamento dei dati, disporre che i trattamenti di dati personali debbano garantire, nell'ambito del sistema articolato organizzativamente come da Atto Aziendale e ulteriori provvedimenti attuativi, il rispetto dei seguenti criteri:

- a) modalità di trattamento che assicurino il rispetto dei diritti e delle libertà fondamentali del cittadino;
- b) operazioni di trattamento espletate nel pieno rispetto delle finalità istituzionali proprie dei compiti affidati a ciascuna struttura;
- c) snellezza e speditezza delle operazioni di trattamento, utilizzando per quanto possibile supporti informatizzati piuttosto che cartacei;
- d) rispetto della tempistica necessaria allo svolgimento delle suddette operazioni, non aggravando inutilmente i procedimenti di trattamento;
- e) valutazione approfondita in ogni circostanza degli interessi contrapposti;
- f) economicità e razionalità nell'utilizzo delle risorse, sempre con lo scopo primario di assicurare il raggiungimento dei risultati;
- g) procedure trasparenti nell'interesse dei cittadini, che devono sapere perché e come sono trattati i dati che li riguardano;
- h) definizione di procedure di verifica periodica circa l'esattezza, l'aggiornamento, la completezza, la pertinenza, la non eccedenza e l'indispensabilità dei dati rispetto alle finalità perseguite nei singoli casi di trattamento;
- i) sviluppo di adeguati strumenti informativi e programmi informatici configurati riducendo al minimo il ricorso a dati personali ed identificativi;
- j) adeguate misure di sicurezza preventive ed idonee a tutela dei trattamenti, mediante opportune misure di protezione e, per i dati su supporto informatizzato e per l'utilizzo delle reti, l'attivazione di sistemi collegati in rete interna ed esterna protetti in modo ottimale rispetto all'evolvere delle tecnologie hardware e software.

#### RESPONSABILI DI TRATTAMENTO.

I soggetti designati "Responsabili del trattamento" sono tenuti a comunicare la propria accettazione secondo le modalità previste nell'atto di nomina, all'uopo predisposto, contenente l'individuazione dei compiti assegnati ed analiticamente specificati per iscritto. I medesimi soggetti dovranno procedere al trattamento dei dati personali attenendosi rigorosamente alle direttive impartite dal titolare con il presente atto di indirizzo e con

eventuali futuri atti. Essi hanno in particolare il compito di concorrere all'aggiornamento periodico del DPS per gli ambiti di rispettiva competenza.

Con riferimento alla possibilità di esternalizzazione di servizi si prevede la designazione, in qualità di "Responsabile di trattamento", di soggetti pubblici e privati che operano per conto del titolare (es. contratti stipulati dall'Azienda, appalti, convenzioni, protocolli, concessioni amministrative, ecc.) relativamente ad operazioni di trattamento strettamente necessarie per l'espletamento dei servizi medesimi.

Menzione particolare tra i responsabili del trattamento merita il dirigente preposto al SISA, che deve garantire la sicurezza degli apparati di rete (fonia e dati), delle banche dati (hardware e software) sia in termini di conservazione dei dati sia di sicurezza contro manipolazioni e/o accessi indebiti.

**Istruzioni di dettaglio sul trattamento dati uniformi per tutte le strutture aziendali e valide per i responsabili e per gli incaricati del trattamento sono contenute nell'allegato sub 3 alle presenti disposizioni.**

#### INDIVIDUAZIONE DEGLI "INCARICATI DI TRATTAMENTO"

Ai sensi e per gli effetti dell' art. 30 del Dlgs. n. 196/2003, chiunque, in ambito aziendale, compie operazioni di trattamento per conto dell' Azienda Sanitaria Locale n. 2 di Olbia è individuato come "incaricato di trattamento", ciascuno nell'ambito delle funzioni e dei compiti specificatamente attribuiti. Il profilo di responsabilità dell'incaricato di trattamento è direttamente connesso ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle proprie mansioni e compiti.

La designazione degli incaricati avviene all'atto dell'instaurazione di qualsivoglia rapporto con l'Azienda, a cura del responsabile del trattamento nel cui ambito organizzativo l'incaricato è inserito o con il quale deve collaborare; con l'atto di designazione, il responsabile del trattamento impartisce le opportune disposizioni operative adattando al caso di specie **lo schema tipo di provvedimento di incarico allegato sub 4** al presente atto di indirizzo; la designazione può essere, altresì, formalizzata in via straordinaria in situazione di urgenza, al momento dell'espletamento delle prestazioni richieste.

Gli incaricati di trattamento operano sotto la diretta autorità dei responsabili ai quali rispondono, attenendosi alle istruzioni operative impartite dagli stessi.

#### REFERENTE AZIENDALE PRIVACY.

Per coordinare i rapporti tra titolare e responsabili del trattamento e per gli ulteriori compiti nel seguito specificati, la Direzione Generale ha individuato, con delibera n. 813 del 20.08.2009, nell'ambito dell'Area Affari Generali, Legali, Comunicazione, una figura, denominata "Referente Aziendale Privacy", alla quale vengono attribuiti I seguenti compiti:

- proporre azioni e adempimenti necessari per l'applicazione della normativa in materia di trattamento dei dati personali con possibilità di segnalazione alla Direzione Generale (es: notificazione dei trattamenti ex art. 37 Dlgs n. 196/2003; comunicazione dei flussi informativi ex art. 39 ecc);
- fornire supporto giuridico ai responsabili del trattamento, se necessario, per la soluzione di quesiti a valenza generale inerenti istanze per l'esercizio del diritto di accesso ai dati personali, ex art. 7 del Codice Privacy, che presentino particolari criticità da risolvere;
- concorrere a programmare le iniziative e le attività di formazione e aggiornamento del personale responsabile del trattamento e preposto allo svolgimento delle operazioni di trattamento;
- predisporre gli atti inerenti la nomina dei responsabili di trattamento e gli schemi tipo di provvedimento a valenza generale (ad esempio, per l'attribuzione degli incarichi di trattamento)
- svolgere funzioni di coordinamento in ordine alla predisposizione ed all'aggiornamento della modulistica contenente l'informativa agli interessati e per l'acquisizione del consenso, di competenza dei responsabili del trattamento;
- seguire l'attività dell'Autorità Garante per la protezione dei dati personali per i necessari aggiornamenti da fornire al titolare e ai responsabili del trattamento, che avranno cura a loro volta di informare gli incaricati del trattamento.

	<b>DIREZIONE</b>
1	Direzione Amministrativa
2	Direzione Sanitaria
3	Area Affari Generali e Legali
4	Area Programmazione, controllo e committenza
5	Servizio di assistenza infermieristica, ostetrica e p.t.s.
6	Integrazione socio – sanitaria
7	Qualità Risk Management
8	Servizio informatico sanitario e amministrativo
9	Servizio Prevenzione e protezione aziendale
10	Formazione
11	Servizio Provveditorato e Amministrazione del Patrimonio
12	Servizio Contabilità e Bilancio
13	Servizio Amministrazione del Personale
14	Servizio Tecnico
15	Servizio Sorveglianza Sanitaria
16	Farmacovigilanza
17	<b>Distretto Olbia</b>
18	Servizio delle cure primarie
19	Servizio specialistica ambulatoriale
20	Servizio assistenza a disabili e soggetti fragili
21	Servizio Assistenza integrata (P.U.A.; U.V.T.; A.D.I.)
22	Servizio dell'assistenza riabilitativa e prestazioni integrative e protesiche
23	Servizio Assistenza farmaceutica territoriale
24	Servizio Consultoriale
25	Servizio di Emergenza ed urgenza territoriale
26	Servizio territoriale di neuropsichiatria infantile e dell'adolescenza
28	<b>Distretto Tempio P.</b>
29	Servizio delle cure primarie
30	Servizio assistenza a disabili e soggetti fragili
31	Servizio Assistenza integrata (P.U.A.; U.V.T.; A.D.I.)
32	<b>Dipartimento di Prevenzione</b>
33	Igiene e Sanità Pubblica
34	Prevenzione e sicurezza negli ambienti di lavoro
35	Igiene degli alimenti e della nutrizione
36	Sanità animale
37	Igiene della produzione, trasform., commercial., conservazione alimenti origine animale
38	Anagrafe zootecnica e coord. Dei piani annuali di risanamento
39	Filiera della macellazione
40	Filiera della pesca
41	Lotta al randagismo
42	Latte e produzione lattiero caseario
43	Vigilanza insediamenti produttivi e prevenzione delle malattie infett.
44	Contr. porti e aereop.arrivo e trans.animali vivi e delle derrate
45	<b>Dipartimento salute Mentale e Dipendenze</b>
46	Servizio psichiatrico ospedaliero di diagnosi e cura
47	Servizio Dipendenze
48	<b>PRESIDIO OSPEDALIERO DI OLBIA</b>
49	P.O. Olbia - Direzione Medica
50	Patologia forense
51	Servizio farmaceutico ospedaliero
52	U.O.Chirurgia
53	CH Colon proctologia
54	CH Urologica



55	Brest Unit
56	U.O. Ortopedia e Traumatologia
57	CH della mano
58	Day Surgery ortopedica e artroscopica
59	U.O. Ostetricia e Ginecologia
60	Percorso nascite
61	CH Ginecologica
62	U.O. Anestesia e Rianimazione
63	Terapia intensiva
64	Coordinamento complesso operatorio
65	Programma trapianti d'organo
66	Coord. Operativo emergenza urgenza intra ed extra ospedaliera
67	U.O. Medicina Interna
68	U.O. Di Medicina d'Urgenza (SOAPI)
69	Day Hospital internistico
70	Gastroenterologia
71	U.O. Cardiologia UTIC
72	Elettrofisiologia
73	Diagnostica cardiologica
74	Scoperto Cardiaco
75	U.O. Pronto Soccorso
76	U.O. Pediatria Neonatologia
77	Assistenza neonatale
78	Diabetologia pediatrica
79	Medicina per immigrati
80	U.O. Oncologia
81	U.O. Nefrodialisi
82	U.O. Neurologia
83	P.O. Olbia - Diabetologia
84	Fisiologia e patologia della nutrizione
85	Laboratorio Analisi
86	Centro Trasfusionale
87	Patologia della coagulazione
88	Autisti
89	Centralino
90	U.O. Di Radiologia
91	Diagnostica ecografico
92	Diagnostica pesante
93	<b>PRESIDIO OSPEDALIERO DI LA MADDALENA</b>
94	P.O. La Maddalena - Direzione Medica
95	U.O. Anestesia e Rianimazione e Terapia Iperbarica
96	U.O. Medicina Interna
97	U.O. Ostetricia
98	U.O. Pediatria a Assistenza neonatale
99	U.O. Pronto Soccorso
100	U.O. Dialisi
101	Dipartimento salute mentale
102	Servizio salute mentale
103	Doppia diagnosi
104	Dipartimento di Prevenzione
105	Igiene e sanità
106	Medicina legale
107	Medicina del viaggiatore
108	Ambiente e salute
109	Promozione ed educazione alla salute
110	Epidemiologia
111	Sicurezza alimentare

112	<b>PRESIDIO OSPEDALIERO DI TEMPIO P.</b>
113	P.O. Tempio Pausania – Direzione Medica
114	U.O. Anestesia e Rianimazione
115	Terapia del dolore
116	U.O. Cardiologia
117	U.O. Chirurgia
118	CH oncologica
119	U.O. - Diabetologia
120	U.O. Dialisi
121	U.O. Fisiatria
122	U.O. Laboratorio Analisi
123	U.O. Medicina Interna
124	Lungodegenza
125	Diagnostica vascolare
126	U.O. Ortopedia e Traumatologia
127	U.O. Ostetricia e Ginecologia
128	Percorso nascite
129	CH Ginecologica
130	U.O. Otorinolaringoiatria
131	Audiologia e vestibologia
132	U.O. Pediatria e Assistenza neonatale
133	U.O. Pronto Soccorso
134	U.O. Radiologia
135	Diagnostica tradizionale ed ecografia
136	Diagnostica pesante

Sub 2

"Allegato alla delibera n° 40  
del 11.01.2010".

**ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI  
(ART. 29 DEL D.Lgs 196 del 30 giugno 2003)**

Il sottoscritto dott. Giovanni Antonio Fadda, nella sua qualità di Commissario e legale rappresentante della Azienda Sanitaria Locale n. 2 di Olbia - Titolare del trattamento dei dati - ai sensi e per gli effetti dell'art. 29 del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali)

**NOMINA**

..... Responsabile del trattamento dei dati nell'ambito dell' Area, struttura, servizio, u.o., articolazione organizzativa.....

In detta veste la S.V. ha il potere/dovere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni in materia di protezione dei dati personali e più in particolare:

- 1) procedere al trattamento dei dati personali attenendosi alle disposizioni di legge ed alle direttive impartite dal titolare da adattare in base all'organizzazione data alla struttura/servizio in cui è preposto;
- 2) nominare gli incaricati al trattamento dei dati, secondo le modalità stabilite dalle disposizioni contenute nelle linee di indirizzo e di programmazione in attuazione del Dlgs. n. 196/2003 impartendo loro precise istruzioni operative nel rispetto delle disposizioni vigenti e dei compiti assegnati;
- 3) definire le procedure di verifica per il trattamento dei dati ed effettuare controlli periodici;
- 4) verificare la qualità e la quantità dei dati oggetto dei trattamenti di competenza con specifico riferimento ai requisiti di indispensabilità, esattezza, aggiornamento, completezza, pertinenza e non eccedenza;
- 5) elaborare l'aggiornamento periodico del Documento Programmatico sulla sicurezza (DPS) per quanto di competenza;
- 6) partecipare ai momenti formativi organizzati dall'Azienda ed assicurare la partecipazione dei propri incaricati.

La presente nomina è inscindibilmente connessa all'incarico di Direzione di Struttura ed è condizionata, per oggetto e durata, all'incarico conferito e si intenderà revocata di diritto alla cessazione del rapporto di lavoro.

**Una copia della presente nomina deve essere restituita, debitamente firmata, all'Area Affari Generali, Legali e Comunicazione.**

“Allegato alla delibera n° 40  
 del 11.01.2010”.

## ISTRUZIONI GENERALI PER IL TRATTAMENTO DISCIPLINARE SULL'USO DI INTERNET E POSTA ELETTRONICA

### Premessa

*Il trattamento dei dati personali deve svolgersi “ nel rispetto dei **diritti e delle libertà fondamentali**, nonché della **dignità** dell’interessato, con particolare riferimento alla **riservatezza**, all’**identità personale** e al diritto alla **protezione dei dati personali**”*

*Da tale enunciazione del Codice della Privacy (D.lgs.196/03) derivano una serie di obblighi in capo a chiunque utilizzi dati personali, non soltanto obblighi di riservatezza e segretezza ma anche di tutela, protezione e sicurezza dei dati.*

*I principi contenuti nel Codice della Privacy devono essere conosciuti e rispettati da chiunque tratti, nell’esercizio delle proprie funzioni, dati e informazioni personali e sensibili.*

*Il presente documento ha lo scopo di agevolare la lettura e l’interpretazione della normativa, dettando le necessarie prescrizioni e fornendo istruzioni operative. Il documento opera nei confronti di ogni dipendente dell’Azienda Sanitaria Locale n. 2 di Olbia e di tutti i soggetti (responsabili ed incaricati) che a vario titolo si trovino ad utilizzare il sistema dell’Azienda.*

*Le istruzioni si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina i rapporti di lavoro.*

### Istruzioni

*Le seguenti istruzioni sono parte del sistema di sicurezza che l’Azienda Sanitaria Locale n. 2 Olbia adotta al fine di gestire, nel rispetto della vigente normativa, i dati trattati.*

*Si sintetizzano di seguito alcuni aspetti particolarmente rilevanti in materia; è comunque indispensabile che chiunque tratti dati personali o sensibili prenda visione del vigente DPS – Documento Programmatico sulla Sicurezza, redatto da tutte le strutture aziendali.*

## 1. Istruzioni in tema di sicurezza

### Documentazione cartacea

- *Il responsabile, l'incaricato, per tutto il periodo in cui effettua le operazioni di trattamento dei dati, non deve mai perdere il dominio sui documenti, adempiendo ad un preciso obbligo di custodia dei medesimi;*
- *Il responsabile, l'incaricato deve predisporre un sistema per controllare che i documenti siano sempre completi ed integri;*
- *in caso di abbandono, anche temporaneo, dell'ufficio, Il responsabile, l'incaricato non deve mai lasciare incustoditi i documenti (sulla scrivania o su tavolini di reparto); è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un locale, un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.); ove si utilizzi un contenitore chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo di soggetti autorizzati;*
- *occorre in particolare accertarsi che nessun visitatore o terzo estraneo (addetto alla manutenzione, alle pulizie, ecc. o un collega non autorizzato) possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti;*
- *al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza (ad esempio, per le spedizioni, l'utilizzo di buste sigillate);*
- *la distruzione dei documenti contenenti dati personali o sensibili deve avvenire con modalità che rendano impossibile l'individuazione dell'utente da parte di terzi non autorizzati.*

### Utilizzo del sistema informatico

- *tutti i dipendenti dell'Azienda e tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale possono essere intestatari di un nome di utente all'interno del dominio di sicurezza aziendale;*
- *tutti gli appartenenti alla suddetta categoria possono avere accesso al servizio di posta elettronica;*

- *tutti gli appartenenti alle suddette categorie possono richiedere l'accesso ad Internet che sarà autorizzato o meno – in base alla mansione e a considerazioni organizzative – dal responsabile del trattamento di riferimento;*
- *la parola chiave di accesso alla postazione informatica e agli applicativi aziendali deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;*
- *la parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato;*
- *a tutti gli utenti del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della parola chiave; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile sostituirla anche prima;*
- *qualora si utilizzino sistemi che non siano in grado di richiedere automaticamente il cambio di password è indispensabile che l'utente – autonomamente - provveda a cambiarla ogni tre mesi*
- *Il responsabile, l'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare;*
- *per gli utenti del dominio aziendale è previsto, in molti casi, un sistema di salvataggio dei files centralizzato, all'interno di file servers; i documenti gestiti all'interno dei file servers sono tutelati da perdite mediante accurate procedure di salvataggio; ove esistenti i server, è fatto divieto di memorizzare in locale sulle stazioni di lavoro dati sensibili, che vanno salvati sui file servers; nel caso in cui l'utente memorizzi anche solo per brevi periodi dati in locale sulla stazione di lavoro, deve procedere con cadenza almeno settimanale all'effettuazione di copie di sicurezza e riporre i supporti di salvataggio in un contenitore sicuro al quale possano accedere esclusivamente soggetti autorizzati*
- *tutti i pc devono avere il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi al Servizio Informativo Aziendale*
- *in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati, ad esempio scollegandosi o attivando un salvaschermo protetto da password*
- ***è vietato l'utilizzo della posta elettronica per l'invio di dati sensibili***

- *è vietato manomettere o cambiare le configurazioni delle attrezzature aziendali se non esplicitamente autorizzati dai competenti servizi*
- *è vietato installare attrezzature non autorizzate e collegarle alla rete aziendale se non dietro esplicita autorizzazione dei servizi competenti*
- *è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia se non espressamente autorizzati o se non previsto dalla propria mansione*
- *per nessuna ragione i dati contenuti e gestiti nel sistema informativo aziendale saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n.300)*

## **2. Istruzioni per l'utilizzo degli strumenti di lavoro**

### **Telefono e fax**

- *nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chiunque risponda all'apparecchio. In caso di risposta negativa è necessario chiedere in alternativa un numero riservato*
- *occorre fare attenzione a discutere, comunicare o comunque trattare dati personali/sensibili per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati*
- *in caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza*
- *qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata*
- *l'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati*

## Fotocopiatrice e stampante

- *in caso di stampa o duplicazione non riuscite di documentazione contenente dati personali / sensibili, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati (mediante apposita macchinetta tritatutto o distruzione manuale in piccoli pezzi)*
- *qualora si utilizzi carta riciclata per fotocopie e stampe, occorre sempre accertarsi che non siano accidentalmente riportati dati personali e/o sensibili*
- *occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso*

## Supporti di memorizzazione

- *è vietato l'utilizzo di supporti rimovibili, come ad esempio floppy disk o cd rom, per lo scambio di dati sensibili; qualora vi fosse assoluta necessità di utilizzarli è indispensabile assicurarsi che essi non vengano riutilizzati e vengano distrutti dopo il loro utilizzo, se vengono riutilizzati occorre verificare che il precedente contenuto sia stato reso assolutamente irrecoverabile – le normali procedure di cancellazione di un dato informatico non sono normalmente sufficienti a garantire ciò, potendosi in molti casi recuperare anche dati cancellati con procedure e strumenti particolari -*



## **Disciplinare sull'utilizzo delle attrezzature aziendali e tenuta di evidenza sull'uso del sistema da parte dell'Azienda.**

- *gli strumenti di comunicazione aziendali e gli strumenti di produttività personale in genere – telefono fisso, telefono cellulare, stazioni informatizzate di lavoro, fax, stampanti, ecc... - concessi in uso dovranno essere utilizzati per fini esclusivamente istituzionali e connessi alla propria mansione e attività di servizio*
- *l'Azienda si riserva di verificare l'utilizzo del telefono e delle stazioni di lavoro informatizzate qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni*
- *l'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso. Il personale tecnico dell'Azienda, o il personale delle aziende che in nome e per conto dell'Azienda effettuano attività di manutenzione sulle attrezzature di produttività personale o sui sistemi di comunicazione potranno accedere agli strumenti di comunicazione o di produttività personale per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto come impedimento all'accesso il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale –*
- *tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log; tali log tengono traccia dei seguenti dati per ogni accesso:*
  - *Indirizzo IP del PC da cui l'utente si è collegato;*
  - *Data e ora*
  - *Riferimento al sito visitato (URL)**Tali log sono indispensabili al SIA – Servizio Informativo Aziendale - per poter costantemente monitorare il corretto funzionamento del sistema e per poter effettuare statistiche periodiche sull'uso del sistema;*
- *l'Azienda si riserva di filtrare l'accesso a siti che risultino non in relazione con le attività istituzionali; il filtraggio verrà attuato mediante l'inserimento del sito in una cosiddetta "Black list"; la lista dei siti inaccessibili potrà essere chiesta alla direzione del Servizio Informativo Aziendale da chiunque e in caso di motivate ragioni potrà essere*

*autorizzata la navigazione sul sito mediante rimozione dalla lista di esclusione; l'esclusione dei siti verrà operata periodicamente in base all'analisi di dati aggregati;*

- *il sistema di posta elettronica tiene traccia di tutte le e-mail inviate e ricevute*
  - *data e ora;*
  - *indirizzo IP del sistema che ha inviato il messaggio;*
  - *indirizzo di posta del mittente;*
  - *indirizzo del destinatario;*
  - *Anche in questo caso i log vengono mantenuti per lo stesso periodo e le stesse finalità indicate per gli accessi Internet;*
  
- *tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail con dei virus, effettua i seguenti controlli:*
  - *blocco delle e-mail con allegati potenzialmente pericolosi (file con estensioni EXE, .COM, .VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK)*
  - *blocco delle e-mail con dimensioni complessive (messaggio di posta + allegati) superiori a 7 Mb.*
  - *blocco delle e-mail con più di 30 allegati e/o più di 50 destinatari.*
  - *In particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il SIA si riserva di bloccare e cancellare le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi.*

*Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in termine tecnico viene chiamato SPAM – l'Azienda ha in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Le regole di filtraggio possono causare;*

- *il passaggio di SPAM qualora non sufficientemente selettive;*
- *il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM.*

*Per le ragioni sopra indicate si vieta l'utilizzo della posta elettronica di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario.*

***Il sistema di posta elettronica in uso, e concesso in utilizzo, non è un sistema di posta certificata, non vi è pertanto la garanzia***

**della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di privacy relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni. È pertanto fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio;**

- *l'Azienda ASL n. 2 di Olbia favorisce la condivisione di indirizzi di posta elettronica fra più utilizzatori mediante l'adozione di cosiddette "maling list", cioè di gruppi di indirizzi;*
- *l'Azienda ASL n. 2 di Olbia non fornirà indirizzi di posta elettronica aziendali per usi di tipo personale, ma non vieta la consultazione del contenuto di indirizzi di tipo personale, anche dall'interno dell'azienda, qualora la modalità di consultazione di tali informazioni sia compatibile con i vincoli di sicurezza del sistema aziendale e ciò avvenga in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda;*
- *l'Azienda mette a disposizione funzionalità di avviso in caso di assenza prolungata del dipendente, che sfruttano le peculiarità del sistema di posta elettronica, e possono fornire coordinate di altri riferimenti all'interno dell'Azienda tali da garantire il corretto funzionamento dei servizi; l'attivazione di tali misure sarà a cura del dipendente che dovrà avvisare le locali sedi del SIA di attuare la misura; qualora il dipendente non abbia adottato tale misura e l'assenza si protragga per più di una settimana, il responsabile del trattamento potrà richiedere al SIA l'adozione di una tale misura;*
- *ogni assegnatario di indirizzo di posta elettronica aziendale potrà, in caso di necessità, dirottare la propria posta elettronica su un diverso indirizzo di posta elettronica personale - o di un fiduciario -; nel caso non sia in grado di attuare detta misura in autonomia, potrà chiedere alla locale sede del SIA la messa in atto della misura; della attuazione di tale misura verrà tenuta traccia e verrà data notizia al lavoratore interessato alla prima occasione utile;*
- *qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'Azienda, occorrerà rendere edotto di ciò il destinatario;*
- *per fini di controllo della spesa telefonica l'Azienda tiene traccia delle telefonate effettuate – qualora queste inducano un onere economico per l'Azienda; non sono ad esempio tracciate le telefonate in ingres-*

*so che sono tipicamente non onerose in termini economici -. Viene registrato:*

- il numero del chiamante;*
  - il numero chiamato;*
  - la data e ora di inizio della telefonata e la data e ora di fine della stessa*
- 
- tutti i log sopra citati vengono conservati dal SIA per un periodo non inferiore ad un anno e non superiore a due; i controlli verranno effettuati in maniera non nominativa e aggregata – ad esempio aggregando i dati per edificio o per unità erogante – qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi potranno essere ulteriormente approfonditi; qualora possibile e sensato, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione; in generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell’Azienda; qualora le verifiche portino all’accertamento della violazione delle presenti regole o più in generale all’accertamento di utilizzi impropri, l’Azienda si riserva di adottare le opportune misure disciplinari e amministrative;*
  - per nessuna ragione i dati informatizzati gestiti dall’azienda, i sistemi di elaborazione dati e gli strumenti di telecomunicazioni saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n.300)*

## ULTERIORI INDICAZIONI OPERATIVE

### Rapporti di front office

- **rispetto della distanza di cortesia:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza
- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazioni di dati (presentate per telefono o via fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario)
- **identificazione dell'interessato e controllo dell'esattezza dei dati:** nel momento della raccolta di dati anagrafici (in particolar modo nel caso di cittadini stranieri) occorre fare attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato
- **la chiamata nominativa dell'utente è vietata :** nelle sale e negli spazi di attesa più affollati occorre utilizzare un numero o altro sistema analogo che prescinda dai dati anagrafici (es. orario della prenotazione).

### Corretta comunicazione dei dati

- **la richiesta di comunicazione o documentazione di dati personali e sensibili può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge (in casi dubbi rivolgere sempre richiesta di chiarimenti al Responsabile)**
- **la comunicazione di dati idonei a rivelare lo stato di salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato dal titolare o dal responsabile**
- **l'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di ri-**

*portare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.*

- ***in ogni caso occorre porre in essere procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparto o strutture indicativa dell'esistenza di un particolare stato di salute.***

Sub 4

"Allegato alla delibera n° 40  
del 11.01.2010".

**ATTO DI NOMINA DI INCARICATO DEL TRATTAMENTO DEI DATI  
PERSONALI (art. 30 del D.Lgs. n. 196 del 30 giugno 2003)**

Il sottoscritto \_\_\_\_\_ direttore dell'Area/struttura/servizio, u.o., articolazione organizzativa \_\_\_\_\_, nominato dal Titolare, nella persona del Commissario, quale Responsabile del trattamento dei dati personali afferenti la suindicata struttura aziendale, ai sensi dell' art. 30 del D.Lgs. 196/2003, con il presente atto

**nomina incaricati**

del trattamento dei dati personali, sensibili e giudiziari raccolti nelle banche dati dell' Azienda Sanitaria (archivi di tipo cartaceo ovvero banche dati elettroniche), in uso presso l' Area/struttura/servizio, u.o., articolazione organizzativa:

- 1) tutti i dipendenti che nelle rispettive funzioni, e nello svolgimento dei compiti specificamente attribuiti hanno ragione di trattare o anche solo accedere ai dati medesimi;
- 2) l' incaricato procederà al trattamento dei dati nel rispetto della normativa vigente e delle seguenti istruzioni operative (specificare distintamente per archivi cartacei e informatici):

3) l'incaricato dovrà effettuare il trattamento dei soli dati la cui conoscenza sia necessaria e sufficiente per svolgimento delle operazioni da effettuare.

4) è compito di ciascun incaricato verificare l'esattezza ed il grado di aggiornamento dei dati trattati;

5) è compito di ciascun incaricato verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile;

6) è compito degli incaricati, ove occorra, di ufficio o ad istanza di parte, provvedere alle correzioni, integrazioni, cancellazioni e aggiornamento dei dati.

**Il nominato sottoscritto prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di incaricato del trattamento dei dati personali.**

Olbia,

Il Responsabile del trattamento dei dati personali

firma \_\_\_\_\_

Per ricevuta

L'incaricato (scrivere nome e cognome in stampatello e poi apporre la propria firma)

COGNOME

NOME

FIRMA

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



---

---

---

---

---

---

---

---

---

---

---

---