SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

COMUNE DI MODOLO

Provincia di Oristano

Documento Programmatico sulla Sicurezza (D.P.S.) relativo ai trattamenti di Dati Personali, Sensibili e Giudiziari

Analisi dei rischi che incombono sui dati trattati dall'Ente e indicazione delle misure da adottare per assicurare l'integrità e la disponibilità degli stessi e per la protezione delle aree e dei locali rilevanti

(Art. 34 D. Lgs. 196/03 - Allegato B al D. Lgs. 196/03, Regola 19)

REVISIONE N° 01
MARZO 2008

CONTENUTO DEL D.P.S.

1. Documento Programmatico sulla Sicurezza redatto ai sensi e per gli effetti dell'allegato B al D. Lgs. 196/2003, che conformemente a quanto previsto dalla Regola 19, il Titolare del trattamento dei dati (l'Ente nel suo complesso con Deliberazione della Giunta) dovrà adottare entro il 31/03/2008. Il presente DPS dovrà essere sottoposto a revisione annuale, con obbligo in capo al titolare del trattamento di riferire dell'avvenuta redazione o revisione nella relazione accompagnatoria del bilancio.
2. Schede di rilevazione ed analisi delle Banche Dati relative ai trattamenti effettuati dall'Ente;
3. Distribuzione dei compiti e delle responsabilità all'interno dell'Ente;
4. Indicazione delle misure di sicurezza già adottate dall'Ente;
5. Illustrazione delle Misure Minime di Sicurezza e delle Misure Idonee da adottare a cura del Titolare e dei Responsabili del Trattamento;
6. Analisi e valutazione dei Rischi;
7. Indicazione dei criteri e delle modalità per il ripristino della disponibilità dei dati personali trattati in seguito a distruzione o a danneggiamento degli stessi;
8. Interventi Formativi;
9. Trattamenti di dati personali affidati all'esterno;
10. Bozza della Deliberazione della Giunta di adozione del Documento Programmatico sulla Sicurezza.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Documento redatto da: **S.I.P.A.L. SRL**

Data di redazione: **17 – 19 Marzo 2008**

COMUNE DI MODOLO

PROVINCIA DI ORISTANO

Documento Programmatico sulla Sicurezza (D.P.S.)
relativo ai trattamenti di
Dati Personali, Sensibili e Giudiziari

Analisi dei rischi che incombono sui dati trattati dall'Ente e indicazione delle misure da adottare per assicurare l'integrità e la disponibilità degli stessi e per la protezione delle aree e dei locali rilevanti

(Art. 34 D. Lgs. 196/03
Allegato B al D. Lgs. 196/03, Regola 19)

REVISIONE N° 01

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

MARZO 2008

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

INDICE

Sezione 7 Descrizione dei Criteri e delle Modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Sezione 8 Previsione di Interventi Formativi

Sezione 9 Trattamento di dati personali affidati all'esterno

Allegato 4 Bozza della Deliberazione della Giunta Municipale di adozione del **Documento Programmatico sulla Sicurezza**.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

1 Premessa

Il Documento Programmatico sulla Sicurezza si inserisce nella disciplina delle misure minime di sicurezza e la sua annuale predisposizione costituisce uno specifico adempimento imposto dall'art 34, comma 1, lett. g) del D Lgs 196/03 e dalla Regola 19 del Disciplinare Tecnico, Allegato B al Codice sulla Privacy

Il presente D.P.S., che costituisce la REVISIONE n. 02 al Documento Programmatico già adottato dall'Ente, può essere definito come il **Manuale della sicurezza fisica e logica dei Sistemi Informativi dell'Ente** in quanto contiene l'esaustiva indicazione e l'attenta analisi dei rischi propri del sistema informatico che ospita dati personali, sensibili e giudiziari trattati dall'Ente e focalizza l'attenzione sull'esame delle contromisure necessarie per contrastare o quanto meno ridurre i citati rischi.

Il D.P.S. mira ad illustrare gli elementi di novità rispetto al passato caratterizzanti il **programma di adeguamento dell' Ente alle Misure di Sicurezza** previste per il trattamento dei dati personali, sensibili e giudiziari così come delineate dal D. Lgs. 196/2003 – Allegato B (Disciplinare Tecnico) nonché alle più ampie misure di sicurezza previste dall'art 31 del citato Decreto

In questa ottica, il D.P.S. rappresenta l'unico strumento efficace mediante il quale l'Ente, è in grado di testimoniare l'applicazione concreta del T.U. Privacy, fornendo attraverso lo stesso, la descrizione ed il censimento aggiornato e puntuale dei dati personali trattati a qualunque titolo per l'espletamento delle finalità istituzionali, l'indicazione delle misure di prevenzione che l'Amministrazione ha adottato e di quelle ancora da adottare, la rappresentazione delle responsabilità legate alla gestione ed al trattamento dei dati, l'individuazione delle attività di formazione, mantenimento e miglioramento necessarie

L'Ente, nel dettaglio, con il presente Documento Programmatico, procede:

1. **alla fedele ricognizione dell'architettura informatica e tecnologica presente e alla descrizione del contesto ambientale in cui i dati sono conservati e custoditi ;**
2. **all'aggiornamento dell'elenco dei trattamenti di dati personali, sensibili e giudiziari effettuati a qualsiasi titolo dai diversi uffici dell'Ente;**
3. **all'indicazione esaustiva della distribuzione dei compiti e delle responsabilità tra i soggetti coinvolti;**
4. **all'indicazione delle misure di sicurezza già adottate;**

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

5. **all'analisi e indicazione compiuta delle misure di sicurezza ancora da adottare;**
6. **all'analisi compiuta dei rischi e delle minacce potenziali e reali che incombono sui dati personali trattati;**
7. **all'individuazione dei criteri e delle modalità di ripristino della disponibilità dei dati;**
8. **alla pianificazione degli interventi formativi previsti per i soggetti individuati quali Responsabili o Incaricati del trattamento dei dati personali;**
9. **alla descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.**

1. **Ricognizione dell'architettura Tecnico – Informatica dell'Ente e del contesto ambientale in cui i dati sono conservati e custoditi**

Sulla base di un attento sopralluogo e di una attività di verifica si procede ad una nuova rilevazione dell'Architettura Tecnologia e Informatica dell'Ente con particolare attenzione rivolta, alla descrizione della tipologia di rete locale presente in Amministrazione che collega tra loro i dispositivi di accesso ai dati utilizzati dagli Incaricati e, all'indicazione delle caratteristiche principali degli strumenti utilizzati per effettuare i trattamenti dai dipendenti.

2. ***Aggiornamento dell'elenco dei trattamenti di dati personali effettuati dall'Ente***

Viene aggiornato e rivisitato il Censimento completo delle Banche Dati contenenti dati personali, sensibili e giudiziari trattati a qualsiasi titolo dagli Uffici dell'Ente, con l'indicazione delle informazioni essenziali per ciascun trattamento e in particolare:

a) la descrizione sintetica del trattamento effettuato dall'Ufficio;
b) l'individuazione della natura dei dati trattati (dati personali, dati sensibili o giudiziari);
c) l'Ufficio di riferimento all'interno del quale viene effettuato il trattamento;
d) la descrizione sintetica della tipologia degli strumenti elettronici utilizzati per trattare i dati.

Le predette informazioni sono contenute all'interno di una tabella idonea a fornire le stesse con riferimento a ciascun Ufficio/Servizio in cui si articola l'organizzazione del Comune.

Ad ogni buon fine giova precisare che, secondo quanto dettato dall'art. 18, comma 2, D. Lgs. 196/03, presupposto generale per la legittimità del trattamento di dati personali da parte di un soggetto pubblico è la necessità del trattamento per lo svolgimento delle funzioni istituzionali proprie del soggetto stesso

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

3. Individuazione dei compiti e delle responsabilità all'interno dell'Ente

In questo capitolo si procede all'individuazione dei compiti e delle responsabilità previste dal legislatore per la gestione delle Banche di Dati e, in particolare, per il trattamento dei dati personali, sensibili e giudiziari con espresso riferimento alle figure del Titolare, dei Responsabili e degli Incaricati del trattamento dei dati.

4. Indicazione delle misure di sicurezza gia adottate dall'Ente

Si procede alla individuazione delle misure di sicurezza già adottate dall'Ente per ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati trattati;
- accesso non autorizzato agli stessi;
- trattamento non consentito o non conforme alle finalità della raccolta.

L'indicazione delle suddette misure di sicurezza già adottate dall'Ente avverrà suddividendo gli interventi effettuati in:

- interventi sulle infrastrutture;
- interventi sugli strumenti e sulla rete informatica;
- interventi sulla organizzazione dell'Ente.

5. Indicazione analitica delle misure di sicurezza che l'Ente deve ancora adottare

In questo capitolo si procede alla completa individuazione delle misure di sicurezza previste dal dettato normativo che l'Ente dovrà provvedere ad adottare con urgenza.

L'indicazione delle citate misure di sicurezza sarà realizzata suddividendo le stesse misure in **Misure Minime di Sicurezza,** in ottemperanza al Disciplinare Tecnico (Allegato B al D. Lgs. 196/03) relativamente ai punti da 1 a 26 e **Misure Idonee,** da adottare sia relativamente alle Banche Dati censite che, in senso più esteso, in relazione all'intero Sistema Informativo dell'Ente ai sensi dell'art. 31 del D. Lgs. 196/03.

6. Analisi dei rischi e delle minacce che incombono sui dati personali trattati

In questa sede si procede alla valutazione delle Minacce Potenziali e Reali, delle Vulnerabilità e del Rischio Residuo che incombono sui dati e più in generale sull'intero Sistema Informativo dell'Ente.

7. Individuazione dei criteri e delle modalità di ripristino della disponibilità dei dati

In questa sezione sono descritti i criteri e le procedure adottati dall'Ente per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità sopraggiunta.

8. Pianificazione degli interventi formativi previsti dall'Ente per i soggetti individuati quali Responsabili o Incaricati del trattamento di dati personali

In questo capitolo sono riportate sinteticamente le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere

9. Trattamenti affidati all'esterno

In questo capitolo si indicano i criteri adottati dall'Ente per garantire il rispetto degli obblighi previsti dal Codice in materia di protezione dei dati personali nelle ipotesi di trattamenti di dati affidati a soggetti esterni

Al fine di rendere più agevole la consultazione e la lettura del presente Documento Programmatico, nella tabella che segue sono indicati, per ciascuna delle **SEZIONI** in cui si articola il Documento, la problematica trattata e la relativa definizione sintetica..

SEZIONE	PROBLEMATICA	DEFINIZIONE
1	Architettura informatica e tecnologica	Indicazione ed analisi della Struttura dell'architettura informatica e tecnologica dell'Ente
2	Elenco dei trattamenti	Elenco Generale dei trattamenti di dati personali effettuati all'interno dell'Ente da parte dei singoli uffici
3	Distribuzione dei compiti	Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposta al trattamento dei dati all'interno del Comune
4	Misure di Sicurezza di cui l'Ente già dispone	Illustrazione delle Misure di Sicurezza già adottate dall'Ente per garantire la Integrità e la Disponibilità dei dati, suddividendo gli interventi effettuati in: • interventi sulle infrastrutture; • interventi sugli strumenti e sulla rete informatica; • interventi sulla organizzazione dell'Ente.
5	Misure di Sicurezza ancora da adottare	Illustrazione delle Misure da adottare per garantire la Integrità e la Disponibilità dei dati, con distinguo tra: • Misure Minime di Sicurezza (Art. 33 e Disciplinare Tecnico – Allegato B al D. Lgs. 196/03); • Misure Idonee (Art. 31)

6	Analisi di Rischi	Valutazione delle Minacce Potenziali e Reali, delle Vulnerabilità e del Rischio Residuo che incombono sui dati e più in generale sull'intero Sistema Informativo dell'Ente
7	Ripristino	Indicazione dei criteri e delle modalità che per garantire il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento degli stessi
8	Formazione	Previsione degli interventi formativi dei responsabili e degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare
9	Soggetti Esterni	Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare

Metodologia per l'Analisi e la Valutazione dei Rischi

L'Analisi e la Valutazione delle Minacce, delle Vulnerabilità e del Rischio residuo da abbattere (Sezione 6) è uno dei temi più importanti di tutto il Programma di adeguamento in quanto l'evidenza del Rischio emergente potrà comportare la necessità di interventi, in taluni casi anche molto onerosi, sulle infrastrutture e sugli apparati informatici del Comune.

Pertanto l'analisi è stata affrontata con approccio molto realistico, evitando in primo luogo di indicare la necessità di proteggersi dal verificarsi di Minacce che presentino una probabilità di accadimento molto bassa che comporterebbero, in conseguenza di una accettazione della gestione del rischio, costi di protezione e tutela molto elevati, non sostenibili finanziariamente dall'Ente.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Inoltre, in considerazione delle esigue risorse finanziarie a disposizione dell'Ente, il metodo adottato per procedere all'analisi e alla valutazione dei rischi è stato quello di agire nel senso del contenimento delle vulnerabilità rispetto alla minacce reali evidenziate, soprattutto sotto l'aspetto organizzativo, procedurale e formativo piuttosto che su quello infrastrutturale e tecnologico, molto più oneroso per l'Amministrazione, introducendo ove possibile misure equivalenti di protezione

Trattamenti effettuati senza l'ausilio di strumenti elettronici

Questa tipologia di trattamenti coincide con i trattamenti di atti e documenti cartacei, in originale ed in copia.

Come per i trattamenti effettuati con strumenti elettronici, le persone che accedono ai dati devono essere preventivamente individuate e potranno svolgere le operazioni di trattamento in qualità di incaricati.

La nomina ad incaricato non comporta l'accesso a tutti i dati cartacei, ma solo a quelli previsti nel profilo di incarico. Tale profilo può essere organizzato per gruppi omogenei di attività corrispondenti alle mansioni svolte in un determinato comparto dell'Ente. L'ambito del trattamento consentito a ciascun incaricato o alle unità organizzative è oggetto di periodici aggiornamenti.

In pericolare, la Regola 27, contenuta nell'Allegato B al D. Lgs. 196/03, prevede che:
"Agli Incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione."

I principi alla base di questa norma sono tre:

1) la sicurezza deve proteggere i dati durante tutte le fasi di lavorazione e durante tutto il loro ciclo di vita, assicurando costantemente la custodia ed il controllo.
2) Solo gli incaricati espressamente designati ai sensi dell'art. 30 D. Lgs. 196/03, possono legittimamente trattare dati.
3) L'ambito del trattamento consentito agli incaricati è verificato con cadenza almeno annuale.

L'insieme di questi principi comporta l'obbligo di impartire agli incaricati istruzioni scritte finalizzate al controllo e alla custodia degli atti e dei documenti loro affidati

L'organizzazione dei profili di accesso e gli aggiornamenti periodici sono finalizzati al rispetto del principio che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.

La distinzione utile per l'individuazione dei profili di incarico per questa modalità di trattamento è la natura dei dati. Sarà perciò necessario individuare i trattamenti di dati sensibili e giudiziari, differenziandoli da quelli comuni, conseguentemente organizzare i singoli profili di incarico o i gruppi omogenei di persone autorizzate alla stessa attività.

L'organizzazione delle misure di sicurezza comporta una preventiva ricognizione dei trattamenti cartacei che può essere fatta congiuntamente a quella per individuare le operazioni svolte con strumenti elettronici, anche per individuarne le correlazioni

Il nuovo testo normativo riconosce la relazione tra incaricati e unità organizzative dell'Ente Di norma nell'ambito dell'articolazione delle attività svolte dall'Ente, sono raggruppate nella stesso settore/servizio/ufficio lavorazioni aventi la stessa finalità. Tutte le risorse umane assegnate alla stessa unità, avendo profili di incarico simili, sono considerate, ai fini dei trattamenti, un gruppo omogeneo Ciò consente di descrivere il profilo dei trattamenti svolti per l'unità organizzativa e di correlarlo a tutte le persone assegnate a quel settore determinato. Le attività, però, non sono mai definitive, ma dinamiche e mutevoli in ragione dell'evoluzione normativa e regolamentare del settore di riferimento. Da ciò discende l'obbligo di verifica periodica e relativo aggiornamento con cadenza almeno annuale

Per quanto riguarda la custodia si precisa che, gli atti ed i documenti affidati agli incaricati per lo svolgimento dei propri compiti non devono restare incustoditi durante il periodo necessario alla loro lavorazione A tal fine il titolare (l'Ente nel suo complesso) è obbligato a prescrivere il rispetto di procedure che garantiscano la protezione dei dati nella loro integrità onde evitare l'accesso agli stessi da parte di persone non autorizzate Al riguardo sarà necessario anche indicare norme scritte per la procedura di smistamento, distruzione e macero dei documenti cartacei attraverso l'adozione del massimario di scarto e la corretta gestione del protocollo generale dell'Ente.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

La protezione dei dati, specialmente se sensibili o giudiziari, riguarda anche la conservazione, che deve avvenire in archivi ad accesso selezionato. Le procedure di accesso a tali archivi sono finalizzate all'identificazione degli incaricati. Infatti, secondo la norma tecnica (punto 29 del disciplinare) "L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Per quanto sopra esposto, atteso che nella gestione quotidiana della documentazione cartacea il distinguo tra archivio corrente e di deposito è, per comodità lavorativa, ridotto a mera definizione, non esistendo locali specifici all'uopo destinati, si renderà necessario prescrivere, fuori dagli orari di lavoro dell'Ente, la chiusura di armadi e cassetti a mezzo di chiavi non universali che dovranno essere custodite da ogni singolo incaricato del trattamento con copia depositata presso ciascun responsabile del trattamento in busta chiusa e sigillata.

Per quanto attiene all'archivio storico si dovrà adottare la rigida procedura prevista dal punto 29 del Disciplinare Tecnico (ALLEGATO "B" al D. Lgs. 196/2003).

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

2. Definizioni

Per fini metodologici, al fine di omogeneizzare il linguaggio con riguardo agli Organi Ispettivi e di Vigilanza al servizio del Garante per la Protezione dei Dati Personali, si riportano, di seguito, le definizioni relative ai termini più comunemente usati nel presente Documento Programmatico per la Sicurezza nel Trattamento dei Dati Personali, Sensibili e Giudiziari

Autenticazione informatica
l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità

Blocco
la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento

Banca Dati
qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Comunicazione elettronica
ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Chiamata
la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale

Comunicazione
il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Credenziali di autenticazione
i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica.

Dato personale
qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi
i dati personali che permettono l'identificazione diretta dell'interessato

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Dati sensibili
i dati personali idonei a rivelare:

- **l'origine razziale ed etnica;**
- **le convinzioni religiose, filosofiche o di altro genere;**
- **le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale;**
- **i dati personali idonei a rivelare lo stato di salute e la vita sessuale.**

Dati giudiziari
i dati personali idonei a rivelare provvedimenti di cui all'art. 3/1°/a – b – c – d – e – f – g – h – i – l – m – n – o – r – s – t – u del D.P.R. 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60-61 del codice di procedura penale.

Dati relativi al traffico
qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione

Dati relativi all'ubicazione
ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.

Diffusione
il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo
il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile

Garante
l'autorità di cui all'art 153, istituita dalla **Legge 675/1996**.

Incaricati
le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato
la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali

Misure minime
il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Parola chiave
componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Posta elettronica
messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza

Sistema di autenticazione informatica
l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

Responsabile
la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Reti di comunicazione elettronica
i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione
trasportato;
R*ete pubblica di comunicazioni*
una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

Servizio di comunicazione elettronica
i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'art. 2/c della Direttiva 02/21/CE del Parlamento europeo e del Consiglio, del 07-mar-2002;

Sistema di autorizzazione
l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Strumenti elettronici
gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

Titolare
la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Trattamento
qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la

modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Utente
qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

SEZIONE **Architettura informatica e tecnologica dell'Ente**

1 **Contesto ambientale in cui i dati sono conservati e custoditi**

Assetto Organizzativo del Comune

Il Comune è organizzato in Settori, Servizi ed Uffici ai quali sono preposti i dipendenti costituenti la dotazione organica dell'Ente. Il personale di ruolo viene in alcuni casi affiancato, nell'esercizio dell'attività istituzionale, da collaboratori a progetto e da consulenti esterni all'uopo incaricati.

Architettura del Sistema Informativo ed Informatico dell'Ente

L'Architettura del Sistema Informativo del Comune è fondamentalmente basata sul modello Punto a Punto (Peer to Peer o LAN PARITETICA).

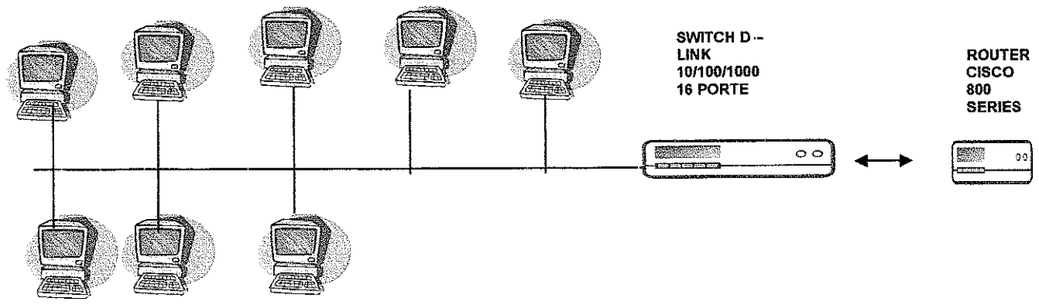
Esiste infatti una piccola infrastruttura di Rete Locale che interconnette le diverse Unità di Elaborazione tra loro basata sul modello ***peer to peer (Punto a Punto)***. Gli elaboratori in uso agli Uffici Comunali sono collegati tra loro in rete ma **non esiste un Server di dominio**

Per la gestione della Rete Locale si rileva la presenza di uno SWITCH con le seguenti caratteristiche tecniche: SWITCH D - LINK DES1218 a 16 porte, con velocità di transito dei dati 10/100/1000.

Nella Rete Locale del tipo Peer to Peer quale quella presente all'interno dell'Ente, non esiste una gerarchia precisa nell'ambito della rete e ogni computer si può indifferentemente comportare sia da server che da client.

Le rete del tipo Peer to Peer è facile da realizzare e far funzionare, ma purtroppo non risulta essere molto affidabile dal punto di vista della sicurezza e dell'amministrazione. Infatti, in una rete locale di questo tipo oltre al fatto che tutte le postazioni possono essere considerate client o server indifferentemente, non esiste un Server di dominio e tutte le postazioni vengono configurate per lavorare in un contesto di Gruppo di Lavoro o WorkGroup.

Ogni utente è anche l'amministratore del proprio client ossia è lui stesso a decidere se condividere o meno una risorsa con gli altri e ad impostare i permessi per quella risorsa (lettura e scrittura, condivisione con password o sola lettura).



Non essendo presente un Server di dominio non esiste una macchina che funga quale unità di autenticazione per verificare l'identità dei Client per l'accesso alla Rete Locale: nessuna password di rete è al momento utilizzata.

Con il Router (CISCO 800 SERIES) residente in Comune, su linea ISDN, tutti gli utenti collegati alla Rete Locale si connettono ad Internet passando attraverso il Server/Router della Comunità Montana VIII **"Marghine Planaria"** su linea ADSL.

La C.M. VIII si trova a Macomer nel Corso Umberto al civico 186. Gli altri Comuni appartenenti alla C.M. VIII sono di seguito indicati: Birori – Bosa - Bortigali – Borore - Bolotana - Bosa - Dulachi – Flussio – Lei - Macomer - Magomadas - Montresta - Noragugume - Sagama - Silanus – Sindia - Suni - Tinnura.

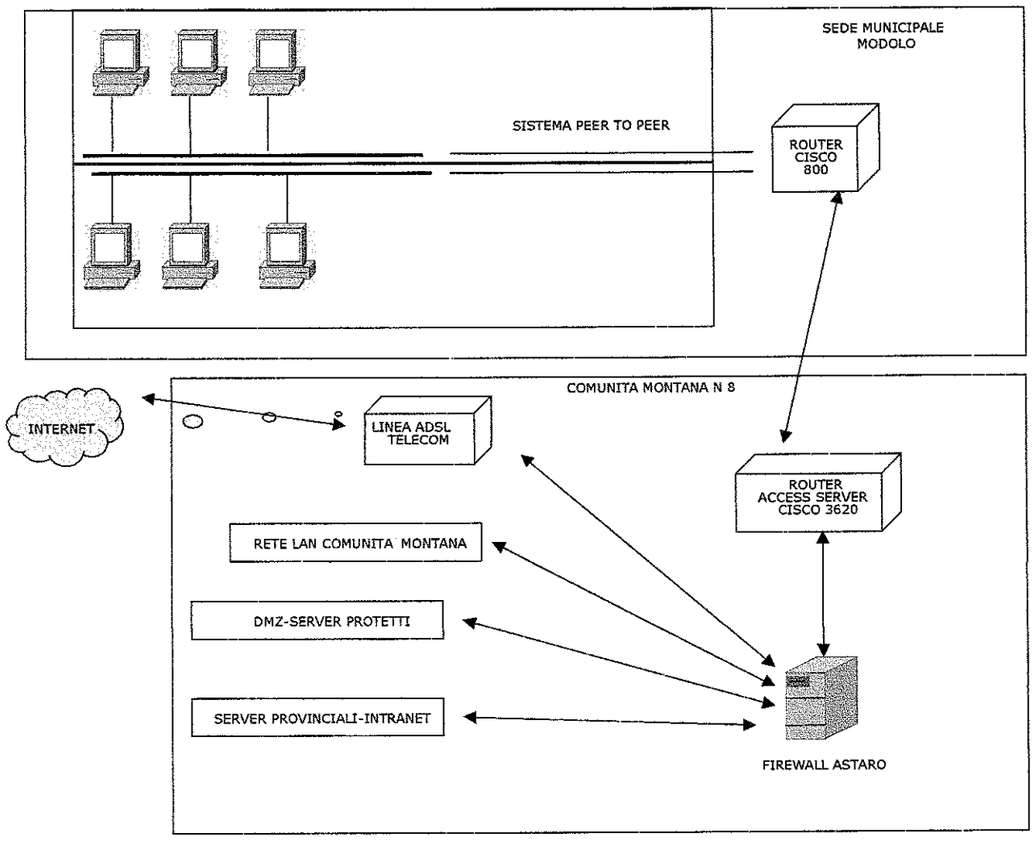
L'accesso ad Internet avviane quindi passando attraverso l'apparato della Comunità Montana. Tramite il Router comunale **Cisco 800 Series** si accede al Server/Router della Comunità Montana (**Access Server 3620)** e successivamente al **Firewall Astaro**. Da qui, si può avere accesso alle seguenti funzionalità:

- al router **ADSL** telecom attraverso cui avviene la connessione ad Internet da parte delle macchine presenti in Comune;
- alla rete LAN della comunità Montana;
- al Server DMZ per Web, posta elettronica e procedure gestionali;
- ai Server provinciali intranet per Web, posta elettronica e procedure gestionali.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

La connessione ad Internet risulta essere adeguatamente protetta grazie alla presenza del Firewall Hardware (ASTARO) presente in Comunità Montana opportunamente configurato con chiusura delle porte logiche: sono state infatti correttamente impostate le regole di filtraggio dei pacchetti di informazioni che transitano nella rete dall'esterno verso l'interno e viceversa



Nell'Ente non è presente un **software Antivirus centralizzato**, residente su Server, che provveda alla distribuzione in tempo reale degli aggiornamenti a tutti gli utenti collegati in rete. Quasi tutti i Pc presenti in casa comunale sono comunque dotati di programmi Antivirus che vengono aggiornati con cadenza periodica codificata in modalità automatica.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Non è presente un back up Server che gestisca in modo automatico le copie dei dati e dei documenti La frequenza con la quale vengono effettuate le copie di sicurezza dei dati non è regolamentata. Ciascun ufficio provvede secondo le proprie esigenze ad effettuare i salvataggi dei dati in modo del tutto autonomo in assenza di qualsivoglia disciplina con cadenza generalmente mensile

I supporti di memoria utilizzati sono rappresentanti da Floppy disk, da DVD ovvero da CD.

I supporti di memoria su cui vengono effettuati i salvataggi, sono custoditi in armadi o cassetti muniti di serratura a cura di ciascun ufficio procedente.

In particolare, l'Ufficio Ragioneria procede mensilmente ad effettuare le copie di sicurezza dei dati ospitati sull'elaboratore utilizzando dei floppy disk come supporti di memoria che poi vengono custoditi all'interno di un cassetto dotato di serratura.

L'Ufficio Servizi Sociali provvede mensilmente ad effettuare il backup dei dati su CD successivamente custoditi in supporti muniti di serratura.

Anche i Servizi demografici, la Polizia Municipale, l'Ufficio Economato, l'Ufficio del Messo comunale, i Tributi, il Commercio ed il Protocollo procedono con cadenza mensile a realizzare le copie di sicurezza dei dati su CD che vengono custoditi all'interno di un cassetto munito di serratura.

Tutti i PC collegati alla Rete Locale Peer to Peer, sono dotati di un gruppo di continuità, per contrastare gli eventuali sbalzi di tensione elettrica

Non è presente un server di posta elettronica. L'Ente non è dotato né di utenze di Posta Elettronica Certificata (PEC) né di Smart Card per la firma digitale.

Si registra una carente gestione del sistema e delle procedure per l'autenticazione informatica.

Infatti, per accedere al proprio PC, non si è ancora provveduto ad attribuire a tutti i dipendenti incaricati del trattamento dei dati, una Credenziale di Autenticazione costituita da una User-Id e da una Password. Inoltre la Password, anche laddove sia stata attribuita, sebbene secondo quanto dispone la norma risulti essere costituita da un numero di caratteri alfanumerici pari almeno ad otto, non sempre viene autonomamente modificata da ciascun utente al primo utilizzo e successivamente con cadenza semestrale ovvero trimestrale nell'ipotesi di trattamento di dati sensibili o giudiziari.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 - 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

I Software gestionali utilizzati sono dotati di regolare licenza d'uso ma non sempre vengono tempestivamente aggiornati ad ogni release del produttore.

Periodicamente si provvede all'installazione degli ultimi aggiornamenti del sistema operativo e delle applicazioni

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

SCHEDA SINTETICA RIASSUNTIVA

CARATTERISTICHE DEL SISTEMA INFORMATICO – TECNOLOGICO DELL'ENTE

Comune di MODOLO – CASA COMUNALE

- All'interno dell'Ente tutti gli elaboratori sono collegati in rete secondo il modello Peer to Peer I Pc dei vari Uffici Comunali sono collegati tra loro in rete ma **non esiste un server di dominio;**
- non essendo presente un Server di dominio, non esiste una unità che proceda alla autenticazione al fine di verificare l'identità dei CLIENT per l'accesso alla Rete Locale.
- l'accesso ad Internet da parte di tutti gli elaboratori della LAN comunale avviene attraverso il Server/Router ADSL. Telecom ospitato presso la sede della C.M. VIII di Macomer al quale ci si collega tramite il Router (CISCO 800 SERIES) residente in Comune, su linea ISDN;
- per quanto rilevato e dichiarato in fase di sopralluogo, in considerazione del fatto che la connessione ad Internet avviene attraverso il Server/Router della C.M. VIII, questa risulta sufficientemente protetta grazie alla presenza di un Firewall Hardware, localizzato presso la Comunità Montana, opportunamente configurato con chiusura delle porte logiche;
- non è presente in Casa Comunale un software Antivirus centralizzato che provveda alla distribuzione in tempo reale degli aggiornamenti a tutti gli utenti collegati in rete; sono tuttavia presenti programmi antivirus in tutti i PC che vengono aggiornati con periodicità codificata in modalità automatica;
- non è presente un back up Server che gestisca in modo automatico le copie dei dati e dei documenti. Ciascun ufficio provvede autonomamente all'effettuazione di copie di backup su CD, Floppy disk DVD con cadenza almeno mensile in assenza di qualsivoglia espressa regolamentazione in materia;
- non si è ancora provveduto ad attribuire la Credenziale di Autenticazione costituita da USER-ID e Password a tutti gli incaricati del trattamento dei dati per l'accesso al proprio PC. Inoltre la Password anche laddove attribuita, non viene modificata autonomamente dall'incaricato al primo utilizzo e successivamente secondo la periodicità codificata dalla Legge (ogni sei mesi ovvero ogni tre mesi nell'ipotesi di trattamento di dati sensibili o giudiziari);
- non è presente un server di posta elettronica. L'Ente non è dotato di utenze di Posta Elettronica Certificata e di Smart Card per la firma digitale;
- tutti gli elaboratori collegati alla Rete Locale comunale sono dotati di gruppo di continuità per contrastare gli eventuali sbalzi di tensione elettrica;

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

- i Software gestionali utilizzati sono dotati di regolare licenza d'uso; non sempre si procede tempestivamente e con regolarità all'aggiornamento in caso di release del produttore;
- periodicamente sono installati gli ultimi aggiornamenti del Sistema operativo e delle applicazioni.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 -- 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

SEZIONE 2 L'Elenco dei Trattamenti di dati personali effettuati dall'Ente

Una attività di attenta ricognizione "in loco" ha consentito di aggiornare, alla luce delle novità intercorse, l'elenco dei trattamenti di dati personali, sensibili e giudiziari svolti all'interno del Comune o all'esterno per conto del Comune stesso, organizzati in raccolte di Banche Dati.

La ricognizione ed il censimento delle Banche Dati e dei Trattamenti sono stati realizzati mediante sopralluoghi effettuati presso ogni singolo ufficio dell'Ente.

Per ogni trattamento è stato specificato:

- Il Settore di riferimento;
- L'ufficio dove le banche dati sono detenute e trattate;
- La denominazione delle Banche Dati;
- La natura dei dati trattati;
- Le tipologie di trattamento;
- I supporti sui quali sono registrati i dati;
- La tipologia dell'unità di elaborazione;
- La sintetica descrizione delle misure di protezione adottate

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

SEZIONE 3 Compiti e responsabilità

In questa sezione si provvede all'esame ed all'elencazione dei compiti e delle responsabilità previste dal legislatore in capo ai soggetti che gestiscono delle Banche Dati e, più in particolare, in capo ai soggetti che trattano dati personali, sensibili e giudiziari con espresso riferimento ai compiti ed alle responsabilità del Titolare, dei Responsabili e degli Incaricati del trattamento nell'Ente Locale.

L'Ente, con Deliberazione della Giunta, provvede ad individuare i Responsabili del Trattamento (coincidenti con i responsabili di Area/Settore/Servizio già esistenti nella pianta organica dell'Ente) e questi, conformemente al disposto normativo, designano con propria determinazione, gli Incaricati del trattamento adottando gli atti di nomina e di designazione allegati alla presente sezione.

L'obbligo di protezione dei dati personali trattati riguarda il Titolare del trattamento, il Responsabile/i, gli Incaricati e più ampiamente chiunque sia tenuto all'adozione di misure di sicurezza, ivi compreso l'Amministratore del Sistema Informatico, che potrà essere interno o esterno all'Ente.

IL TITOLARE DEL TRATTAMENTO

Ai sensi dell'art. 4, comma 1, lett. f) D. Lgs. 196/03, per Titolare si intende:
"la persona fisica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza."

L'art. 28 del Codice precisa che:
"Quando il trattamento è effettuato da una persona giuridica, da una Pubblica Amministrazione o da qualsiasi altro ente, titolare del trattamento è l'entità nel suo complesso che esercita ( )"

Un recente Provvedimento del Garante per la Protezione dei Dati Personali, del 14/06/07 (G.U. n. 161 del 13/07/07), recante "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", precisa definitivamente che in ambito pubblico "per individuare il Titolare del trattamento, occorre far riferimento all'amministrazione o ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'Amministrano o la rappresentano (ad esempio, il ministro, il direttore generale o il presidente).

Il Titolare è dunque l'Ente nel suo complesso e non i singoli soggetti fisici che operano al suo interno. Sarà dunque l'Ente, che dovrà adempiere alle disposizioni contenute nel Codice sulla Privacy.

Al Titolare spettano le decisioni strategiche in materia di sicurezza nel trattamento dei dati anche qualora vengano nominati, per fini pratico – operativi, dei Responsabili.
Il Titolare è il centro di imputazione degli obblighi e delle responsabilità attribuite dalla legge.
Egli ha il compito, e i compiti del Titolare NON SONO DELEGABILI, di organizzare e vigilare sull'intero processo di trattamento dei dati. Egli è il destinatario delle sanzioni previste per il mancato rispetto delle relative norme: è una figura necessaria perché non ci può essere un trattamento di dati senza che vi sia un corrispondente Titolare

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Il Titolare:

- Può individuare uno o più responsabili affidando loro compiti ANALITICAMENTE specificati PER ISCRITTO. La designazione deve essere espressa: non può essere considerato Responsabile un soggetto senza che vi sia un atto formale di designazione o di nomina;
- Deve redigere, anche eventualmente con l'ausilio dei Responsabili, entro il 31 Marzo di ogni anno, un Documento Programmatico sulla Sicurezza, secondo quanto stabilito dalla Regola 19 dell'Allegato B al D. Lgs. 196/063;
- Deve effettuare verifiche periodiche;
- Vigilare puntualmente sull'osservanza delle disposizioni di legge e delle proprie istruzioni.

Ricordiamo infatti che, se il titolare del trattamento (l'Ente locale nel suo complesso) designa uno o più responsabili non sarà esonerato dagli obblighi di sicurezza perché, ai sensi dell'art. 29 del Codice, dovrà impartire per iscritto analitiche istruzioni per l'effettuazione del trattamento ed avrà l'obbligo di vigilare anche attraverso verifiche periodiche, sulla puntuale osservanza delle disposizioni e delle proprie istruzioni rispondendo inoltre per "culpa in eligendo" e per "culpa in vigilando".

IL RESPONSABILE DEL TRATTAMENTO

Secondo quanto disposto dall'art. 4, comma 1, lett.g) del Codice, per Responsabile si intende:
"la persona fisica (..) preposta dal Titolare al trattamento dei dati personali".
Questo significa che, mentre il Titolare esiste indipendentemente da qualsiasi atto di nomina, il Responsabile del Trattamento esiste solo se il Titolare del Trattamento (l'Ente nel suo complesso) esercita una delle facoltà ad esso concesse dalla Legge.

Recita infatti l'art. 29 del Codice che:
"il Responsabile è designato dal Titolare facoltativamente".
La nomina del Responsabile è pertanto facoltativa ma, allorquando il Titolare (l'Ente nel suo complesso sulla base di una deliberazione della Giunta Comunale) decida di procedere alla sua individuazione, sarà necessario che la scelta ricada su un soggetto che presenti caratteristiche di "esperienza, capacità ed affidabilità" e che "garantisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."
Il fatto che la norma si preoccupi di dare delle indicazioni sulle caratteristiche soggettive e, in parte, professionali del soggetto da nominare quale Responsabile del trattamento ha un duplice significato. Da un lato essa tende a garantire che la tutela della riservatezza venga demandata a soggetti con determinate capacità ed esperienze. Dall'altro lato, essa indica il metodo per evitare che il Titolare incorra in quella che viene definita "culpa in eligendo", ossia un colposo errore di scelta che, oltre a rendere assolutamente INVALIDA la nomina, avrebbe anche l'effetto di ricondurre "in toto" ogni responsabilità in capo al Titolare.

Oltre ad avere i requisiti ora citati, la nomina del Responsabile deve seguire i criteri di forma stabiliti dalla norma

In primo luogo la nomina deve avvenire con ATTO SCRITTO in cui vengono elencati specificamente i compiti assegnati al responsabile del trattamento.

Infatti, anche se l'atto scritto non risulta espressamente previsto dal legislatore, la necessità di produrre un atto scritto con l'indicazione della nomina del responsabile e dei compiti ad esso assegnati, è evidente dalla lettura del comma 4, dell'art. 29 del Codice, che stabilisce che "i compiti affidati al Responsabile devono essere analiticamente specificati per iscritto".

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Inoltre il comma 5, dello stesso art. 29, stabilisce che "il Responsabile procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza (..) delle proprie istruzioni". E' importante sottolineare che i Responsabili possono essere più di uno

Il Responsabile è per definizione il soggetto "preposto" dal Titolare al trattamento di dati personali. Se ne deduce che il responsabile nominato potrebbe occuparsi di tutte le fasi che costituiscono il trattamento medesimo e anche di più trattamenti Ciò deve essere visto alla luce di quanto riportato nel Mansionario redatto dal Titolare all'atto della nomina del responsabile.

Le funzioni e l'ambito di operatività del Responsabile possono essere individuate solo attraverso le indicazioni fornite dal Titolare.

GLI INCARICATI DEL TRATTAMENTO

Gli incaricati del trattamento sono definiti come "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

A differenza dei Responsabili, figure sicuramente eventuali, non è immaginabile un trattamento di dati personali senza Incaricati del trattamento medesimo: essi devono esistere necessariamente in qualsiasi realtà operativa Infatti secondo l'art. 30 del Codice, "le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite."

Devono essere nominati quali Incaricati del trattamento dal Titolare o dal Responsabile tutti i soggetti che, nella pratica, raccolgono i dati, li elaborano, li archiviano, li comunicano, li diffondono ecc.
In base a quanto disposto dall'art. 30, "la designazione degli Incaricati deve avvenire per iscritto e deve individuare puntualmente le operazioni del trattamento consentite all'incaricato "

Ai sensi della citata norma, è di fatto indispensabile che siano nominati Incaricati tutti i soggetti che in qualsiasi modo effettuano una o più operazioni nell'ambito del trattamento.
E' bene tenere presente che gli Incaricati nominati, possono effettuare solo le operazioni nei limiti di cui alla loro nomina e sotto il diretto controllo del Titolare o del Responsabile. Ciò significa prima di tutto che, come per la nomina del Responsabile, anche per gli Incaricati, deve essere redatto un apposito Mansionario attraverso il quale vengono fornite all'operatore tutte le indicazioni necessarie affinché egli operi correttamente negli ambiti consentiti

Al fine di poter correttamente definire gli ambiti di competenza e responsabilità dei soggetti individuati quali Titolare, Responsabili e Incaricati del trattamento dei dati nell'Ente, rimettiamo, nell'Allegato 1, i Modelli di Assegnazione degli incarichi a Responsabili e Incaricati del trattamento dei dati personali adottati dall'Ente.

COMPITI E RESPONSABILITA'

L'obbligo di sicurezza riguarda il Titolare del trattamento, i Responsabili, gli Incaricati e più ampiamente, chiunque sia tenuto all'adozione o al rispetto di misure di sicurezza all'interno dell'Ente.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Le misure adottate dovranno proteggere i dati personali e i sistemi, quindi i programmi informatici, gli strumenti elettronici utilizzati, il sistema informativo nel suo complesso, gli atti ed i documenti cartacei, gli ambienti nei quali vengono svolte le operazioni di trattamento, ivi compresi gli archivi.
Così come per il Titolare anche per il Responsabile infatti, vige l'obbligo di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati ivi compreso il profilo della sicurezza

Ricordiamo ancora che il Titolare, ha l'obbligo di vigilare affinché le istruzioni impartite al Responsabile, comprese quelle sulla sicurezza, siano rispettate, e ciò tramite verifiche periodiche prescritte al comma 5 dell'art. 29 del Codice.

Pertanto da parte del Titolare e del Responsabile dovrà essere svolta in modo continuativo un'azione formativa nei confronti degli Incaricati del trattamento affinché, ai sensi dell'art. 31 del Codice, si concretizzi il pieno rispetto del disposto normativo che testualmente recita: "i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"

L'Ente, nell'adottare le idonee misure di sicurezza, dovrà tener conto di quanto previsto dall'art. 15 del Codice per effetto del quale, il danno (anche non patrimoniale) cagionato a terzi per effetto del trattamento di dati personali, dovrà essere risarcito secondo quanto previsto dall'art 2050 c c e cioè a meno che non si fornisca in giudizio la prova volta a dimostrare di aver adottato tutte le misure idonee ad evitare il danno.

Il citato articolo 15 ha un rilievo straordinario.
Il legislatore infatti, nella considerazione che l'attività di trattamento dei dati, sia ormai divenuta tanto utile ed indispensabile alla collettività, la eleva al rango di "attività pericolosa" e, in quanto tale, pretende che chiunque realizzi delle ipotesi di trattamento di dati adotti tutte le prudenze e le idonee misure di sicurezza preventive, necessarie ed opportune.

Il Titolare ed il Responsabile, perciò, dovranno adottare le più **idonee misure** di prevenzione, oltre a quelle **minime prescritte**, tra quelle disponibili in relazione alle conoscenze acquisite e allo sviluppo delle tecnologie, allo scopo di ridurre al minimo i rischi, possibili, probabili, prevedibili e prevenibili che incombono sui dati. Le scelte operate, sulla base dell'articolato del Codice, determineranno effetti diversi ai fini dell'eventuale risarcimento del danno prodotto a terzi o dell'applicazione di sanzioni penali o di ammende.

L'omessa adozione delle misure minime, infatti, è punita ai sensi dell'art. 169 del Codice con l'arresto sino a due anni o con l'ammenda da diecimila a cinquantamila euro.

L'inosservanza delle norme sulla sicurezza nel trattamento dei dati, potrà comportare responsabilità civili e penali da parte del titolare, del responsabile o di chiunque, essendovi tenuto, ometta di adottarle o di osservarle.
In particolare, la **mancata adozione delle misure minime di sicurezza**, integra, oltre ai profili di responsabilità civile, anche il reato di cui all'art. 169 D Lgs. 196/03, ed è quindi penalmente sanzionata.
Il reato di cui all'art. 169, comma 1, del Codice, si caratterizza come reato omissivo proprio che si consuma a prescindere dal verificarsi di un evento dannoso, con l'inizio del trattamento non accompagnato dall'adozione delle misure minime prescritte.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 -- 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

L'omessa adozione delle necessarie **misure idonee** e preventive comporta invece, ai sensi dell'art. 15 D. Lgs. 196/03, la responsabilità civile di chi ha cagionato danni patrimoniali o non patrimoniali ad altri per effetto del trattamento.

Un ulteriore aspetto da valutare riguarda il concetto di **idoneità delle misure di sicurezza**. Dalla lettura dell'art. 31 del Codice emergono alcuni concetti utili per la valutazione dell'idoneità delle misure idonee che devono garantire la custodia ed il controllo dei dati trattati.

Il principio di base riguarda la conoscenza e la necessità di adeguarsi a quanto proposto in materia di sicurezza nel trattamento dei dati dall'evoluzione tecnologica.
La previsione del legislatore non può che riferirsi alle conoscenze generali di cui dispone la cultura della sicurezza in un dato momento storico, oltre alle esperienze acquisite. Questo, nella pratica di tutti i giorni, indipendentemente dalle misure minime, suggerisce l'opportunità di adottare adeguate e idonee misure organizzative, gestionali, tecniche, fisiche e logiche, tenendo conto dell'evoluzione tecnologica intervenuta e dell'esperienza maturata nella materia

Un secondo principio, correlato a quello di base appena visto, riguarda la nozione di "misure di sicurezza", che nella sua formulazione esprime un concetto "dinamico" e non "statico", proprio perché richiede una ricognizione sempre aggiornata sulle possibili soluzioni tecniche da adottarsi per garantire per la sicurezza Il dettato legislativo, in un certo senso, pretende il meglio, pur considerando la gradualità temporale concessa per l'adozione delle misure stesse

Il titolare, che ricordiamo in Pubblica Amministrazione deve essere inteso come l'Ente Locale nel suo complesso, fermo restando l'obbligo di adottare le misure minime indicate nel Codice, è relativamente libero di stabilire cosa si intende per misure protettive idonee e di adottarle, ma le scelte fatte potranno costituire oggetto di valutazione in caso di contenzioso o di interventi ispettivi.

Il titolare che tratta dati personali in modo lecito e sicuro deve organizzare la loro protezione non solo con le misure di sicurezza minime e più ampie ma anche governando tutti gli altri processi che, sinergicamente, accompagnano il ciclo di vita dei dati.

Tale ricognizione, sulla base delle prescrizioni contenute nel disciplinare tecnico, è svolta dall'Ente con cadenza annuale e viene riportata in questo documento programmatico della sicurezza della cui revisione o aggiornamento il Titolare del trattamento riferirà nella relazione accompagnatoria del bilancio.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Allegato 1 Modelli di Assegnazione degli incarichi a Responsabili e Incaricati del trattamento dei dati personali

DELIBERAZIONE DELLA GIUNTA COMUNALE PER L'INDIVIDUAZIONE DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

COMUNE DI
Provincia di

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

A) DELIBERAZIONE N. del

OGGETTO : Adempimenti di cui al D. Lgs. n. 196/2003 – Declaratoria inerente la responsabilità del trattamento dei dati – Individuazione dei Responsabili del trattamento dei dati personali.

LA GIUNTA COMUNALE

Premesso che:

- in data 01 01 2004 è entrato in vigore il nuovo codice in materia di protezione dei dati personali D. Lgs 196/03, che ha recepito ed innovato la precedente legislazione in materia e che prescrive numerosi e complessi adempimenti;

- ai sensi del combinato disposto di cui agli artt 4, comma 1, lett. f) e 28, comma 1, del D. Lgs. 196/03 quando il trattamento dei dati è effettuato da una Pubblica Amministrazione il **Titolare del trattamento** è **"l'entità nel suo complesso"** e che pertanto titolare del trattamento dei dati personali gestiti dagli uffici del Comune è il Comune medesimo;

- **nel Provvedimento a carattere generale del Garante per la Protezione dei dati personali del 14/06/07 (G.U. n. 161 del 13/07/07)** rubricato "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" viene definitivamente chiarito che **il Titolare del trattamento dei dati in Pubblica Amministrazione è l'Amministrazione ovvero l'Ente Locale nel suo complesso, anziché le singole articolazioni interne ovvero le persone fisiche che l'amministrano o la rappresentano.**

Rilevato che:

- l'art 4 del D. Lgs. 196/03 definisce il Responsabile del trattamento come colui che è preposto dal Titolare al trattamento di dati personali;

- l'art. 29, comma 2, 3, 4 e 5 del citato Decreto, dispone che:

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

"Se designato, il Responsabile del trattamento è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza
Ove necessario per esigenze organizzative, possono essere designati Responsabili più soggetti, anche mediante suddivisione dei compiti.
I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal titolare.
Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare

Considerato, ai sensi delle norme citate, che la complessità dei compiti affidati e la organizzazione dell'Ente giustificano l'individuazione di più Responsabili del trattamento, con specificazione analitica dei compiti e delle responsabilità affidati.

Ritenuto che per l'ambito di attribuzioni, funzioni e competenze conferite, i Responsabili di Area/Settore abbiano i requisisti di esperienza, capacità e affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, compreso il profilo della sicurezza, per cui gli stessi devono essere individuati come responsabili del trattamento limitatamente alle competenze afferenti alle proprie unità organizzative e ciascuno per i trattamenti e per gli adempimenti riguardanti l'Area/Settore cui sono preposti.

Osservato che i poteri dei Responsabili del trattamento dei dati (tra gli altri, quello di incaricare altri soggetti al trattamento) sono coerenti con i poteri conferiti ai responsabili di Area/Settore.

DELIBERA

1. di individuare, per le motivazioni e con le precisazioni espresse in parte narrativa, quali Responsabili del trattamento dei dati personali, i singoli Responsabili di Area/Settore ciascuno per i trattamenti e per gli adempimenti riguardanti l'ambito cui sono preposti nei limiti delle funzioni ed istruzioni di cui all'Allegato A alla presente deliberazione (di cui fa parte integrante e sostanziale);

2. di dare mandato al Sindaco pro tempore di formalizzare con apposito decreto sindacale la designazione dei Responsabili del trattamento dei dati e, secondo quanto indicato nel citato Allegato A alla presente, l'esatta individuazione dei compiti loro affidati;

3. di ratificare le designazioni precedentemente operate dal Sindaco con Decreto Sindacale n del ;

4. di dare mandato all'Ufficio Personale di inserire un rinvio alla presente deliberazione, con specifico riferimento all'Allegato A, per i futuri decreti sindacali di nomina di Responsabili di Area/Settore, che così verranno pertanto contestualmente incaricati anche della responsabilità del trattamento dei dati;

5. di demandare ai Responsabili del trattamento dei dati, come sopra individuati, la nomina, con proprio atto, degli Incaricati del trattamento secondo quanto previsto dall'art 30 D. Lgs. 196/03;

6. che siano designati, di norma, quali ulteriori Responsabili del trattamento dei dati personali, i soggetti esterni all'Amministrazione comunale che abbiano l'incarico di gestire Servizi e conseguentemente effettuare trattamenti di dati di cui il Comune sia titolare. Tale designazione ed individuazione sarà effettuate direttamente in convenzione, nel contratto o nel provvedimento di attribuzione dell'incarico, tramite rinvio alla presente deliberazione.

La suddetta designazione dovrà contenere:

a) l'indicazione nominativa del soggetto esterno all'Amministrazione da individuare quale Responsabile del trattamento dei dati, qualora si tratti di persona fisica;
b) l'individuazione della persona giuridica, della Pubblica Amministrazione o di qualsiasi altro Ente qualora Responsabile del trattamento dei dati esterno all'Amministrazione comunale sia una persona giuridica, un'altra Pubblica Amministrazione o qualsiasi altro Ente;

7. di allegare alla presente deliberazione l'Allegato A contenete l'indicazione del ruolo, delle funzioni e delle istruzioni per i soggetti individuati ai sensi del presente atto come Responsabili del trattamento dei dati ai sensi del richiamato art. 29 D. Lgs. 196/03.

Con separata ed unanime votazione, la presente deliberazione viene dichiarata immediatamente eseguibile ai sensi dell'art. 134, comma 4°, del D.Lgs. 18 agosto 2000, n. 267

ALLEGATO A
Ruolo, funzioni ed istruzioni per i soggetti individuati dall'Amministrazione Comunale quali Responsabili del trattamento dei dati ai sensi dell'art. 29 D. Lgs. 196/03

Nello svolgimento dell'incarico affidato, ciascun Responsabile del trattamento, individuerà e nominerà con proprio atto gli Incaricati del trattamento del settore di pertinenza, impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati.

In particolare, ciascun Responsabile del trattamento dei dati, è responsabile:

1. della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
2. dell'informativa da rendere all'interessato prima di procedere alla raccolta dei dati ai sensi dell'art. 13 D. Lgs. 196/03;
3. dell'effettuazione del censimento e monitoraggio delle tipologie di dati e delle banche dati di pertinenza del settore di propria competenza (distinguendo se si tratti di dati gestiti su supporto cartaceo, informatico o su entrambi i supporti e distinguendo se si tratti di dati personali o di dati sensibili o giudiziari);
4. del controllo affinché il personale facente capo al servizio di propria pertinenza si attenga, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e affinché vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
5. dell'adozione delle misure di sicurezza da introdurre nell'ambito del trattamento dei dati o, qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente ai sensi del Titolo V del Codice Privacy;
6. dell'emanazione, per iscritto, di direttive e ordini di servizio al personale addetto al proprio settore, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali, sensibili e giudiziari;

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

7. della vigilanza sul rispetto del D. Lgs. 196/03 da parte degli incaricati del trattamento nominati in particolare per quanto attiene la corretta e lecita raccolta dei dati, l'utilizzazione, la comunicazione e la diffusione degli stessi anche mediante Pubblicazione in Albo Pretorio;
8. del rispetto della riservatezza nell'ambito dei procedimenti di accesso ai documenti di pertinenza del suo ufficio secondo quanto previsto dalla vigente normativa e dal Regolamento Comunale che disciplina l'accesso agli atti ed ai documenti amministrativi;

Inoltre, ciascun Responsabile del trattamento dei dati:

- evade tempestivamente le eventuali richieste di informazione da parte dell'Autorità Garante e rende immediatamente esecutive le eventuali indicazioni che dovessero pervenire dalla medesima Autorità;
- vigila sulla puntuale evasione delle istanze presentate dall'Interessato ai sensi dell'art 7 D. Lgs 196/03;
- provvede, su richiesta dell'Interessato, ad aggiornare, modificare o integrare i dati personali.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C F e P I. 02848400921
C S. € 90.000,00 (i.v.)
REA 228746

DECRETO SINDACALE DI NOMINA DEL/I RESPONSABILE/I DEL TRATTAMENTO DEI DATI

Decreto Sindacale n del

Oggetto: atto di nomina dei responsabili del trattamento dei dati personali ai sensi e per gli effetti dell'art 29 D. Lgs. 196/03

IL SINDACO

CONSIDERATO che:

1. il 1 gennaio 2004 è entrato in vigore il nuovo codice in materia di protezione dei dati personali D Lgs.196/03, il quale detta gli adempimenti da porre in essere in materia da parte delle PP. AA.;
2. l'art. 28 del D. Lgs 196/03 prevede che allorquando il trattamento dei dati sia effettuato da una Pubblica Amministrazione il Titolare del trattamento è "l'entità nel suo complesso", perciò nel caso di specie il Comune;
3. nel Provvedimento a carattere generale del Garante per la Protezione dei dati personali del 14/06/07 (G U n. 161 del 13/07/07) rubricato "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" viene definitivamente chiarito che il Titolare del trattamento dei dati in Pubblica Amministrazione è l'Amministrazione ovvero l'Ente Locale nel suo complesso, anziché le singole articolazioni interne ovvero le persone fisiche che l'amministrano o la rappresentano;
4. l'art. 4 del D. Lgs 196/03 definisce il Responsabile del trattamento come colui che è preposto dal Titolare al trattamento di dati personali;
5. l'art. 29, comma 2, 3, 4 e 5 del citato Decreto, dispone che:
   "Se designato, il Responsabile del trattamento è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza
   Ove necessario per esigenze organizzative, possono essere designati Responsabili più soggetti, anche mediante suddivisione dei compiti.
   I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal titolare
   Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare.

DATO ATTO che:

1. La Giunta, con propria Deliberazione N del ha ritenuto opportuno prevedere, per la complessità dei compiti affidati e per l'organizzazione propria dell'Ente, l'individuazione di più Responsabili del trattamento, con specificazione analitica dei compiti e delle responsabilità affidati;
2. nella Deliberazione di Giunta di cui al precedente punto, viene stabilito di individuare quali Responsabili del trattamento dei dati personali i singoli Responsabili di Area/Settore ciascuno per i trattamenti e per gli adempimenti riguardanti l'ambito cui sono preposti;
3. nell'Allegato A alla richiamata Deliberazione la Giunta stabilisce in maniera analitica il ruolo, le funzioni e le istruzioni da assegnare ai soggetti individuati quali Responsabili del trattamento dei dati;
4. con il medesimo atto di Giunta si delibera di dare mandato al Sindaco pro tempore di formalizzare con apposito decreto la designazione dei Responsabili del trattamento dei dati e l'esatta individuazione dei compiti loro affidati in conformità a quanto stabilito nell'Allegato A alla Deliberazione di Giunta

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 -- 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

DECRETA

di nominare, per le motivazioni espresse in premessa, quali Responsabili del trattamento dei dati personali i dipendenti aventi la qualifica di Responsabile di Area/Settore ciascuno per i trattamenti e per gli adempimenti riguardanti il servizio cui sono preposti secondo quanto riportato nello schema che segue:

RESPONSABILE DEL SERVIZIO	DENOMINAZIONE DEL SERVIZIO

In caso di assenza temporanea per congedo ordinario, per ferie o per altre cause di breve durata dei dirigenti e/o funzionari sopra indicati, le relative responsabilità e compiti, saranno assunte dai responsabili di procedimento.

Nello svolgimento dell'incarico affidato, ciascun Responsabile del trattamento, individuerà e nominerà con proprio atto gli Incaricati del trattamento del settore di pertinenza, impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati.

In particolare, ciascun Responsabile del trattamento dei dati, è responsabile:

9. della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
10. dell'informativa da rendere all'interessato prima di procedere alla raccolta dei dati ai sensi dell'art. 13 D. Lgs. 196/03;
11. dell'effettuazione del censimento e monitoraggio delle tipologie di dati e delle banche dati di pertinenza del settore di propria competenza (distinguendo se si tratti di dati gestiti su supporto cartaceo, informatico o su entrambi i supporti e distinguendo se si tratti di dati personali o di dati sensibili o giudiziari);
12. del controllo affinché il personale facente capo al servizio di propria pertinenza si attenga, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e affinché vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
13. dell'adozione delle misure di sicurezza da introdurre nell'ambito del trattamento dei dati o, qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti dell'Ente ai sensi del Titolo V del Codice Privacy;
14. dell'emanazione, per iscritto, di direttive e ordini di servizio al personale addetto al proprio settore, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali, sensibili e giudiziari;
15. della vigilanza sul rispetto del D. Lgs 196/03 da parte degli incaricati del trattamento nominati in particolare per quanto attiene la corretta e lecita raccolta dei dati, l'utilizzazione, la comunicazione e la diffusione degli stessi anche mediante Pubblicazione in Albo Pretorio;

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

16. del rispetto della riservatezza nell'ambito dei procedimenti di accesso ai documenti di pertinenza del suo ufficio secondo quanto previsto dalla vigente normativa e dal Regolamento Comunale che disciplina l'accesso agli atti ed ai documenti amministrativi;

Inoltre, ciascun Responsabile del trattamento dei dati:

- evade tempestivamente le eventuali richieste di informazione da parte dell'Autorità Garante e rende immediatamente esecutive le eventuali indicazioni che dovessero pervenire dalla medesima Autorità;
- vigila sulla puntuale evasione delle istanze presentate dall'Interessato ai sensi dell'art. 7 D. Lgs. 196/03;
- provvede, su richiesta dell'Interessato, ad aggiornare, modificare o integrare i dati personali.

_____, li _____

Il Sindaco

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

DETERMINAZIONE PER L'INDIVIDUAZIONE DEGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI E LA DEFINIZIONE DELLE MISURE DI SICUREZZA.

Oggetto: nomina degli incaricati del trattamento dei dati personali preposti alla istruzione dei procedimenti amministrativi dell'Ufficio ………

IL RESPONSABILE DEL TRATTAMENTO DEI DATI DEL SETTORE ……………

Premesso che:

- Con decreto sindacale n° del il Sindaco *pro tempore,* all'uopo delegato dalla Giunta, ha individuato il sottoscritto quale Responsabile del trattamento dei dati per il Settore ………………
- Il D. Lgs. 196/03 impone che all'interno di ogni Pubblica Amministrazione sia costituita una gerarchia, comprendente le figure del Titolare, dei Responsabili e degli Incaricati del trattamento;
- L'art 30 del citato Decreto prevede che le operazioni di trattamento possano essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite;
- Lo stesso art 30 D Lgs 196/03 prevede che la designazione degli incaricati sia effettuata per iscritto e con l'individuazione puntuale dell'ambito di trattamento consentito;

DETERMINA

di designare quali incaricati del trattamento dei dati personali, sensibili e giudiziari contenuti nelle Banche Dati e negli archivi dell'Ufficio ……… i Sigg.ri

………

…………………………………………………… dipendenti assegnati all'ufficio che, in relazione ai compiti loro affidati, vengono a contatto nelle diverse fasi procedimentali con tali informazioni

Con il presente atto di designazione, viene conferito l'incarico di effettuare il trattamento dei dati personali e vengono fornite le opportune istruzioni.

In ottemperanza al D. Lgs 196/03, che regola il trattamento dei dati personali ed in relazione al presente atto di nomina, le SS. LL. sono incaricate di trattare i dati personali, i dati sensibili ed i dati giudiziari necessari per l'espletamento delle diverse fasi procedimentali di competenza nell'ambito dell'Ufficio ………………… secondo le indicazioni di seguito dettagliate.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

I dipendenti individuati quale incaricati dovranno:

1. trattare tutti i dati personali di cui vengano a conoscenza nell'ambito dello svolgimento delle proprie mansioni in modo lecito e secondo correttezza;
2. effettuare la raccolta, l'elaborazione, la registrazione, la consultazione, il raffronto e gli altri trattamenti indicati dal D. Lgs. 196/03 esclusivamente per lo svolgimento di funzioni istituzionali;
3. verificare, ove possibile, che i dati personali siano esatti e, se necessario, provvedere ad aggiornarli;
4. verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile del trattamento;
5. accedere unicamente alle banche dati di competenza dell'Ufficio ..... strettamente necessarie per l'espletamento di funzioni istituzionali;
6. custodire e controllare i dati personali affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
7. evitare di creare banche dati nuove senza autorizzazione del Responsabile del trattamento dei dati;
8. mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza in occasione dell'esercizio delle proprie mansioni;
9. conservare i dati rispettando le misure di sicurezza predisposte dall'Ente

Si precisa inoltre che, i soggetti designati come "incaricati del trattamento" possono accedere comunque ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti ed alle funzioni loro assegnate

Alla luce di quanto esposto, in caso di allontanamento anche temporaneo dal posto di lavoro, l'incaricato dovrà verificare che non vi sia la possibilità da parte di terzi, anche se dipendenti dell'Ente, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato

Nessun dato potrà essere comunicato a terzi, nell'esercizio del diritto di accesso agli atti o diffuso in seguito a pubblicazione in albo pretorio senza la preventiva autorizzazione del responsabile del trattamento.

_____ , addì _____

Il responsabile del trattamento dei dati personali

_____

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Vademecum da consegnare a tutti i dipendenti individuati come Incaricati del trattamento dei dati contestualmente all'atto di nomina

VADEMECUM PER I DIPENDENTI SULL'USO CORRETTO DEGLI STRUMENTI INFORMATICI AI SENSI DEL D. LGS. 196/03

PREMESSA

Definizioni tratte dal Codice della Privacy

- "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza

Il Dipendente

ha diritto al rispetto della riservatezza, ai sensi delle seguenti fonti normative:

- Costituzione, art. 15, 35, 36;
- Statuto dei Lavoratori (L. 300/70) - art. 4: divieto di controlli a distanza dell'attività dei lavoratori, e conseguenti sanzioni penali (art. 38) in caso di violazione del precetto.
- Testo Unico sulla Privacy, D. Lgs 196/03: rispetto di determinati criteri guida, in caso di trattamento di dati personali

L'Ente

- Ha il diritto e il dovere di esercitare i poteri organizzativi del datore di lavoro (art. 41 della Costituzione Italiana), e di organizzare la propria attività in modo da avere sempre piena conoscenza e consapevolezza dell'utilizzo fatto degli strumenti elettronici in proprio possesso assegnati o anche solo utilizzati dai propri dipendenti;
- Considerato altresì che l'Ente risponde in sede civile e penale per l'inosservanza delle disposizioni normative si precisa che grava sullo stesso l'obbligo di verificare, tramite i Responsabili di Area allo scopo individuati e nei limiti consentiti dalle norme, l'osservanza delle norme e dei precetti contenuti nel presente documento o derivanti dalla normativa in vigore

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

TUTTO CIÒ PREMESSO

IL PERSONALE DIPENDENTE DELL'ENTE IN RELAZIONE ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI ASSEGNATIGLI PER LO SVOLGIMENTO DELLE MANSIONI ATTRIBUITE E' TENUTO AL RISPETTO DELLE SEGUENTI REGOLE

Utilizzo della Stazione di Lavoro

- è vietata la installazione e l'utilizzo di programmi di sistema, applicativi e gestionali privi di regolare contratto di licenza d'uso sottoscritto dall'Ente, salvo specifica autorizzazione in tal senso da parte del Responsabile;
- non è consentito modificare le configurazioni (in modo particolare l'identificativo in rete del proprio PC) impostate dall'Amministratore di Sistema;
- non è consentita l'installazione sul proprio PC di dispositivi hardware personali (modem, schede audio, ecc), salvo specifica autorizzazione in tal senso da parte del Responsabile;
- è fatto obbligo al dipendente in possesso di software antivirus di mantenere sempre attivo il programma con riferimento all'ultima versione disponibile. In caso di impossibilità ad operare in questo senso, è necessario fornire immediata segnalazione al proprio Responsabile;
- e' fatto obbligo al dipendente di proteggere la propria stazione di lavoro con una password all'accensione conforme alle prescrizioni contenute nel Documento Programmatico sulla Sicurezza adottato dall'Ente o, in assenza, nella Regola del Disciplinare Tecnico allegato al D. Lgs. 196/03.

Rete Locale e collegamento ad Internet

- è vietato l'accesso e l'utilizzo delle risorse di rete in assenza di preventiva autenticazione informatica da parte dell' Unità di Elaborazione allo scopo preposta
- è vietato l'utilizzo di modem per l'accesso ad Internet, salvo specifica autorizzazione in tal senso da parte del Responsabile;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Ente

Utilizzo dei Supporti Magnetici o Ottici

- non è consentito scaricare files (programmi, archivi di dati, ecc) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
- è fatto obbligo di sottoporre a controllo preventivo tutti i files di provenienza incerta o esterna, attinenti l'attività lavorativa

Navigazione in Internet

- non è consentito navigare in siti non attinenti l'attività lavorativa;
- non è consentita l'effettuazione di transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attenenti l'attività lavorativa o direttamente autorizzati dal Responsabile;
- non è consentito lo scarico di software gratuiti (freeware, shareware, public domain, ecc) salvo casi di comprovata utilità (es. antivirus) ed in ogni caso previa autorizzazione in tal senso da parte del Responsabile;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano attinenti all'attività lavorativa;

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

- non è permessa la partecipazione a Forum e/o l'utilizzo di chat se non per motivi strettamente attinenti allo svolgimento delle mansioni assegnate.

Utilizzo della Posta Elettronica

- non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, Forum o mail-list, salvo specifica autorizzazione in tal senso da parte del Responsabile;
- è sconsigliato e quindi da evitare, l'apertura di allegati di non comprovata origine in assenza di software antivirus aggiornati sulla propria Stazioni di Lavoro;
- è sconsigliato e quindi da evitare la chiamata a link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati;
- è sconsigliato e quindi da evitare il download di file con estensioni: .vbs, .bat, .exe o file e successiva esecuzione delle macro in esso contenute;
- è sconsigliato e quindi da evitare la risposta ad e mail pervenute da mittenti sconosciuti. Si suggerisce, nel dubbio, di cancellarle preventivamente;
- è sconsigliato e quindi da evitare l'invio di allegati in formato Ms-Word (estensione doc): utilizzare in alternativa il formato RTF (estensione .rtf);
- è sconsigliato e quindi da evitare l'invio e l'accettazione anche in sola lettura di messaggi formato html

AVVERTENZA

Quelli sopra elencati rappresentano soltanto alcuni dei precetti che possono essere dettati in questa materia soprattutto in considerazione del fatto che ci si trova ad operare in un contesto estremamente mutevole.

Il dipendente dovrà sempre e comunque conformarsi al seguente precetto di validità generale:

- Gli strumenti informatici assegnati (personal computer, dispositivi e relativi programmi e/o applicazioni) devono essere sempre utilizzati con cura e diligenza;

- Gli strumenti elettronici affidati in consegna o anche solo utilizzati dal dipendente sono strumenti di lavoro dell'Amministrazione, pertanto:
  1. vanno custoditi in modo appropriato, onde evitarne il furto, il danneggiamento o lo smarrimento e, al verificarsi di tale eventualità, deve essere avviata la procedura di denuncia presso le Autorità Competenti;
  2. possono essere utilizzati solo per fini professionali (in relazione , ovviamente alle mansioni assegnate) non anche per scopi personali.

La non osservanza delle Regole sopra elencate potrà comportare sanzioni disciplinari, civili e penali.

F.TO
IL RESPONSABILE DEL TRATTAMENTO DEI DATI

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 4 Misure Di Sicurezza già Adottate Dall'Ente

CASA COMUNALE

Infrastrutture

- ⇨ Sono presenti grate metalliche alle finestre situate al piano terreno della Casa Comunale.
- ⇨ Gli Uffici dell'Ente contenenti fisicamente le banche dati personali sono protetti con sistemi antincendio regolarmente manutenzionati (estintori).
- ⇨ I locali nei quali viene effettuato il trattamento di dati personali sono dotati di pompe di calore.
- ⇨ Al fine di evitare danni ai dati personali trattati nell'ipotesi in cui venga a mancare l'erogazione della corrente elettrica, tutti gli elaboratori collegati alla Rete Locale, sono dotati di gruppo di continuità

Strumenti - Rete LAN / Internet - Antivirus

- ⇨ L'accesso ad Internet avviene attraverso il Server/Router **ospitato presso la sede della C.M. VIII di Macomer su linea ADSL**; la connessione ad Internet risulta sufficientemente protetta grazie alla presenza di un Firewall Hardware, localizzato presso la Comunità Montana, opportunamente configurato con chiusura delle porte logiche.
- ⇨ Nonostante manchi una gestione centralizzata del Software Antivirus, ciascun PC ospita il proprio software che viene regolarmente aggiornato con periodicità codificata in modalità automatica.

Organizzazione

- ⇨ Sono programmati Corsi di Formazione in materia di Privacy e di Sicurezza Informatica rivolti a tutti i Dipendenti e agli Amministratori.
- ⇨ I Software gestionali utilizzati sono dotati di regolare licenza d'uso.
- ⇨ Si provvede ad installare periodicamente e con tempestività gli ultimi aggiornamenti del sistema operativo e delle applicazioni (Service pack, Patch)

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 5 L'Analisi e la valutazione dei rischi e delle minacce che incombono sui dati personali

Il fine delle misure di sicurezza è la protezione dei dati. I dati devono essere integri, disponibili quando necessario e conosciuti solo da chi ha il diritto di accedervi
Per garantire queste qualità è necessario conoscere ed analizzare i rischi che potrebbero inficiarle.

L'Ente è consapevole del fatto che sui dati personali, sensibili e giudiziari oggetto di trattamento da parte degli incaricati incombono una serie di **"minacce potenziali e reali"**

Tali minacce intese come azioni, accidentali o volontarie, di natura ambientale, tecnologica o umana, potrebbero determinare la compromissione di una o più delle qualità fondamentali che viceversa i dati personali oggetto di trattamento debbono sempre possedere e cioè:

a) la **disponibilità**, che assicura che l'accesso ai dati sia disponibile quando necessario e che si ottiene impedendo che l'accesso alle informazioni o alle risorse sia negato senza autorizzazione;
b) l'**integrità**, che garantisce della accuratezza e della completezza dei dati contenuti all'interno degli elaboratori o sui supporti magnetici o ottici e che si ottiene impedendo che le informazioni siano modificate senza autorizzazione;
c) la **riservatezza**, che garantisce che i dati siano conosciuti ed accessibili solo ed esclusivamente dal personale autorizzato e che si ottiene impedendo che le informazioni siano rivelate senza autorizzazione.

A tal fine l'Ente ha condotto un'Analisi del Rischio che si è svolta attraverso i seguenti passi:

1. Ricognizione dettagliata delle Banche Dati trattate a qualsiasi titolo dall'Ente con particolare riferimento al contesto tecnologico e ambientale nel quale il trattamento viene posto in essere anche in ordine alla eventuale presenza di misure preventive e protettive già adottate dall'Ente;

2. Identificazione delle Minacce Reali e Potenziali che incombono sui dati, sugli strumenti e sugli ambienti di cui sopra;

3. Identificazione delle vulnerabilità, cioè delle debolezze o criticità relative al contesto in cui operano o sono conservati i dati e gli strumenti utilizzati per i trattamenti

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 -- 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

L'Analisi dei Rischi è stata condotta con approccio di tipo "qualitativo" piuttosto che "quantitativo" in quanto in quest'ultimo caso si sarebbe avuta la necessità di procedere ad una misurazione "scientifica" degli eventi, con sofisticati calcoli probabilistici Viceversa, in considerazione delle dimensioni strutturali dell'Ente, del contesto ambientale e tecnologico (e nella consapevolezza delle difficoltà oggettive di reperire e censire tutte le informazioni necessarie per procedere secondo questo secondo tipo di approccio), si è scelto appunto di privilegiare l'approccio di tipo "qualitativo", altrettanto efficace in relazione agli scopi prefissati e peraltro in piena coerenza con le indicazioni in tal senso fornite del Garante.

La **Fase 1** ha consentito di rilevare e censire in modo analitico tutte le Banche Dati possedute e trattate dal Comune con l'evidenza delle seguenti informazioni principali:

- ⇨ L'ufficio ovvero il Settore/Area di Riferimento nel quale la Banca Dati viene detenuta e trattata;
- ⇨ La denominazione della Banca Dati;
- ⇨ La Natura dei dati trattati;
- ⇨ Le tipologie di trattamento poste in essere;
- ⇨ Gli Strumenti utilizzati per il trattamento;
- ⇨ I supporti sui quali sono registrati i dati;
- ⇨ La tipologia dell'unità di elaborazione;
- ⇨ La sintetica descrizione delle misure di Prevenzione e Protezione.

Nella **Fase 2** sono state rilevate una serie di minacce potenziali e reali gravanti sui dati, riconducibili ai seguenti principali contesti:

- ⇨ Ambiente fisico all'interno del quale è **allocato** l'hardware o i supporti magnetici o magneto-ottici che contengono i dati Dopo aver individuato i luoghi in cui si svolge il trattamento dei dati e l'esatta ubicazione in cui si trovano i sistemi di elaborazione e di conservazione degli stessi, è possibile classificare alcuni elementi di rischio come, per esempio, possibili intrusioni, eventi naturali, furto, accesso di personale non autorizzato, impossibilità di controllare l'accesso ai locali ecc
- ⇨ Risorse Hardware o supporti magnetici o magneto-ottici che **contengono** i dati ed il software operativo e gestionale che li elabora. Elementi di rischio da considerare che possono minacciare le risorse hardware possono individuarsi in un uso non autorizzato dell' hardware, nella manomissione, nel furto, negli eventi naturali.

- ⇨ Risorse Software operative e gestionali che **trattano** i dati. Con riferimento a queste risorse, gli elementi di rischio vanno ricercati nella possibilità di accesso non autorizzato alle Banche Dati, nella presenza di codici non conformi alle specifiche del programma, nella mancanza degli aggiornamenti del software ecc.
- ⇨ Reti di trasmissione attraverso le quali "**viaggiano**" le richieste di trattamento dei dati e i dati stessi;
- ⇨ Personale che **tratta** i dati;
- ⇨ Procedure per l'accesso alle risorse ed ai dati alle quali **si conforma** il personale che tratta i dati.

Le minacce potenziali, così rilevate, sono state più semplicemente ricondotte ai seguenti tre **ambiti** principali:

- ⇨ **Infrastrutturale;**
- ⇨ **Strumentale;**
- ⇨ **Organizzativo**.

Le minacce reali sono quelle che, tra le minacce potenziali prese in esame, hanno una probabilità di accadimento maggiore all'interno dell'Ente.

Nella **Fase 3** sono state rilevate, per ciascuno degli **ambiti** o contesti analizzati, le specifiche **vulnerabilità**, intese come debolezze intrinseche derivanti dalla assenza o dalla inadeguatezza delle seguenti categorie di elementi di ambito infrastrutturale, strumentale o organizzativo:

- ⇨ **collocazione geografica;**
- ⇨ **caratteristiche hardware;**
- ⇨ **procedure organizzative;**
- ⇨ **misure di sicurezza già adottate**.

Le minacce reali per ciascun **ambito** sono state poste in correlazione con le vulnerabilità presenti nel medesimo contesto e si è valutato il livello di vulnerabilità di tale minaccia. La minaccia è infatti una potenziale causa di un evento dannoso al patrimonio Informativo ed Informatico dell'Ente. La tabella rappresentata in allegato riporta la correlazione **Vulnerabilità del Contesto - Minaccia Potenziale-Evento Dannoso**.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Dalle correlazioni riportate nella tabella, allegata al presente documento per farne parte integrante e sostanziale, abbiamo valutato il **Rischio Residuo** cui sono esposti sia il Sistema Informativo dell'Ente, sia il Sistema Informatico che le singole Banche Dati trattate.

Il Rischio Residuo è stato valutato in termini di:

✓ accettabilità;

⊘ non accettabilità.

con il seguente significato:

✓ accettabilità

riferita sia a basse probabilità di accadimento della minaccia-evento dannoso, che a contenute vulnerabilità di contesto.

In questo caso si ritiene che le contromisure di natura ambientale o tecnico-informatiche già adottate, unitamente a quelle di tipo organizzativo e procedurale, già adottate o da adottarsi, possano essere sufficienti per gestire il Rischio Residuo.

⊘ non accettabilità

riferita sia a medio-alte ovvero medie probabilità di accadimento della minaccia-evento dannoso che ad un livello medio-alto di vulnerabilità di contesto.

La gravità della minaccia unita alle vulnerabilità rilevata è tale per cui ci si trova di fronte ad un Rischio Residuo talmente elevato da gestire con assoluta immediatezza, attraverso l'adozione di misure di sicurezza sia minime che idonee escludendo tassativamente deroghe di alcun genere.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 5.1 Commento alla Tabella di Correlazione Minacce - Vulnerabilità e Rischio Residuo (Allegato 3)

⇨ il rischio legato a **fattori infrastrutturali** e ambientali è intrinsecamente connesso alla struttura fisica degli Edifici dell'Ente ed al complesso delle reti tecnologiche e dei sistemi di prevenzione e protezione già in esercizio in conformità al disposto del D. Lgs 626/94.

⇨ Le minacce che provengono dal **contesto tecnologico e strumentale** incontrano molte vulnerabilità che possono essere ricondotte ai seguenti ambiti:

- obsolescenza ed inadeguatezza tecnologica degli strumenti;
- inadeguatezza formativa;
- inadeguatezza del personale preposto alla gestione del sistema e delle reti

⇨ Le minacce che provengono dal **contesto organizzativo** incontrano molte vulnerabilità di tipo procedurale, oltrechè formativo ed in generale di non diffusa cultura della sicurezza nel trattamento dei dati;

In sintesi ne deriva che, senza un adeguato processo di introduzione di una cultura organizzativa e gestionale sulla sicurezza dei dati ed una conseguente attività di formazione continua, nessun intervento infrastrutturale, tecnologico ed organizzativo potrà ridurre il rischio derivante da una condotta umana errata.

L'Ente, consapevole di queste criticità, in ottemperanza alla norma, si impegna ad adottare specifiche Misure di Sicurezza sia Minime che Idonee dettagliatamente descritte nella successiva Sezione 6.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 6 Misure di Sicurezza da adottare dall'Ente per garantire la integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali in cui questi sono conservati e custoditi – Allegato B al D. Lgs. 196/03 Regola 19.4

La presente sezione descrive le **Misure di Sicurezza** che saranno adottate a cura del Titolare del trattamento dei dati e dei Responsabili designati, per la gestione dei Rischi individuati nella Valutazione di cui alla precedente Sezione.

Le Misure di Sicurezza da adottare saranno di due tipologie:

⇨ **Misure Minime di Sicurezza**, in ottemperanza al Disciplinare Tecnico relativamente ai punti da 1 a 26;

⇨ **Misure Idonee**, da adottare sia relativamente alle Banche Dati censite che, in senso più esteso, in relazione all'intero Sistema Informativo dell'Ente ai sensi dell'art. 31 del D. Lgs 196/03.

Sezione 6.1 Misure Minime di Sicurezza Art 33 D. Lgs. 196/03 – Disciplinare Tecnico (Allegato B al D. Lgs. 196/03) Regole da 1 a 26

Misure minime di Sicurezza (Art. 33 D. Lgs. 196/03 e Disciplinare Tecnico)

Secondo quanto previsto dall'art. 4, comma 3, lett. a) D Lgs. 196/03, per **Misure Minime** si intende "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31"

La sicurezza viene dunque considerata come l'insieme di soluzioni tecniche, informatiche, organizzative, logistiche e procedurali necessarie per ridurre al minimo i rischi di distruzione o perdita dei dati trattati. La sicurezza non è perciò intesa come un mero fatto tecnico

Le misure minime di sicurezza sono puntualmente identificate da parte del Legislatore a causa della previsione della sanzione penale per la loro mancata adozione che vincola al rispetto del principio di tassatività della sanzione penale.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 -- 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

In via prioritaria l'Ente procederà all'adozione delle seguenti **Misure Minime Di Sicurezza** previste dal Codice sulla Privacy agli articoli 33 e 34 e dal Disciplinare Tecnico nei punti da 1 a 26 e non ancora rese pienamente operative all'interno degli Uffici dell'Amministrazione.

Saranno prescritte per tutte le Banche Dati contenenti informazioni di natura personale, di natura sensibile e di natura giudiziaria, le seguenti Misure Minime di Sicurezza in aderenza al disposto normativo.

D. Lgs. 196/03 - Art 34 comma 1. lett. a) e b): autenticazione informatica, procedure di gestione delle credenziali di autenticazione.

Allegato B - Disciplinare Tecnico - Punti 1, 2 e 3

Il trattamento di dati personali con strumenti elettronici è consentito esclusivamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le suddette credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo soggetto.

Ad ogni incaricato sono assegnate una o più credenziali per l'autenticazione

Misura da adottare dall'Ente

La misura comporta che gli utenti del sistema che svolgono una o più operazioni di trattamento siano stati preventivamente individuati e incaricati.
A tali incaricati sono fornite idonee credenziali per l'autenticazione della loro identità (parole chiave, codici di accesso, smart card) riferite all'accesso di un solo specifico trattamento o a più trattamenti, oppure a determinate operazioni di un trattamento.
Il sistema informatico sarà preventivamente impostato per consentire l'associazione delle credenziali a specifici trattamenti, insieme di operazioni o insieme di trattamenti.
Il riconoscimento da parte del sistema delle credenziali permette il superamento della procedura di autenticazione.

Si procederà a prevedere come obbligatorio, per l'accesso agli strumenti elettronici contenenti dati personali, l'uso corretto, il mantenimento e la gestione del sistema di credenziali costituito da:

- USER ID -- CODICE IDENTIFICATIVO DELL'UTENTE
- PASSWORD - PAROLA CHIAVE

Unitamente a ciò:

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

dovranno essere stabiliti i criteri per l'assegnazione delle credenziali agli incaricati Ad ogni incaricato dovrà essere assegnata in busta chiusa la coppia di credenziali di autenticazione costituita da USER ID + PASSWORD per l'accesso ai dati
Ogni incaricato potrà ricevere più coppie di credenziali.

D. Lgs. 196/03 - Art 34 comma 1, lett. b): adozione di procedure di gestione delle credenziali di autenticazione

Allegato B - Disciplinare Tecnico - Punto 4

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Misura da adottare
La norma obbliga il Titolare a impartire istruzioni agli Incaricati con la prescrizione dell'elencazione delle cautele da adottare per garantire la segretezza della componente riservata della credenziale

All'atto della consegna formale delle credenziali di autenticazione all'incaricato si provvederà a notificare allo stesso i criteri da seguire per la corretta gestione delle credenziali ricevute In particolare è fatto obbligo di:
- Evitare di trascrivere la credenziale in fogli "volanti";
- Evitare di digitare la componente riservata della credenziale in presenza di terzi.

D. Lgs. 196/03 - Art 34 comma 1, lett. a) e b): autenticazione informatica, adozione di procedure di gestione delle credenziali di autenticazione

Allegato B - Disciplinare Tecnico . Punto 5

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri alfanumerici oppure, nel caso in cui il sistema operativo non lo permetta, da un numero di caratteri pari al massimo consentito dallo stesso

La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato

Misura da adottare

La lunghezza minima della Parola Chiave è stata scelta dal Legislatore sulla base di calcoli matematici per migliorarne la sicurezza.
Non viene indicato con esattezza dalla norma come deve essere composta la Parola Chiave ma viene

negata la possibilità di utilizzare parole facilmente individuabili da malintenzionati come ad esempio il proprio nome o quello di un familiare del soggetto interessato.

All'atto della consegna formale delle credenziali di autenticazione all'incaricato si provvederà a notificare allo stesso, i criteri con i quali deve essere definita la parte riservata della credenziale di autenticazione Si riportano, a titolo esemplificativo e non limitativo, alcuni criteri derivanti dalla buona pratica:

- non usare il proprio nome, cognome o parti di essi;
- non usare il nome del coniuge, dei figli, dei genitori, la targa della propria autovettura, il codice fiscale o combinazioni di essi;
- non usare date facilmente collegabili: data di nascita, data del matrimonio, etc;
- non usare nomi presenti nel vocabolario italiano o di altre lingue;
- non invertire la parole (es. servizi = izivres);
- non utilizzare parole, termini di uso diffuso e familiare, anche se non presenti in vocabolario;
- utilizzare tutte le posizioni consentite dal Sistema per definire la parte riservata;
- utilizzare insieme numeri, caratteri minuscoli e maiuscoli;
- evitare di ripetere caratteri in posizioni adiacenti;
- Fare ricorso, ove possibile, per facilità mnemonica a parole chiave ricavate da frasi lunghe, composte da numeri, caratteri minuscoli e maiuscoli.

D. Lgs. 196/03 - Art 34 comma 1, lett. b): adozione di procedure di gestione delle credenziali di autenticazione

Allegato B - Disciplinare Tecnico . Punto 5

La parola chiave, quando è prevista dal sistema di autenticazione, sarà modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi In caso di trattamento di dati sensibili o giudiziari sarà modificata ogni tre mesi

Misura da adottare

La durata di una parola chiave non può essere superiore a sei mesi.
Il termine massimo per la modifica è dimezzato per i trattamenti di dati sensibili e giudiziari perché tali dati richiedono protezioni e garanzie maggiori.

Dovrà essere definita nel sistema informatico, con l'assistenza di un soggetto competente a tale scopo incaricato, e con l'ausilio di idonei programmi, la procedura per la gestione in forma automatica dell'obbligo di modifica immediata e successivamente con periodicità semestrale (ovvero trimestrale nel caso di trattamenti di dati sensibili e giudiziari) della parola chiave.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I 02848400921
C S € 90.000,00 (i.v.)
REA 228746

D. Lgs. 196/03 - Art 34 comma 1, lett. b): adozione di procedure di gestione delle credenziali di autenticazione

Allegato B - Disciplinare Tecnico - Punti 6,7,8

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica

Le credenziali sono disattivate anche in caso di perdita della qualità che consentono all'incaricato l'accesso ai dati personali.

Misura da adottare

Sarà necessario, anche attraverso l'assistenza di un soggetto competente a tale scopo incaricato, che sul sistema informatico sia formalmente introdotto il divieto di riutilizzare, anche in tempi diversi, la parte non riservata della credenziale di autenticazione, cioè della USER ID. Questa misura è indispensabile al fine di poter gestire con univocità l'associazione dei codici per l'identificazione ad un solo soggetto al fine di esaminare gli accessi dubbi e sospetti.

Sarà inoltre necessario, anche attraverso l'assistenza di un soggetto competente a tale scopo incaricato, osservare le seguenti prescrizioni:

- cancellazione dell'account di un incaricato, previa segnalazione in tal senso del Responsabile, nei casi di cessazione dal servizio, mobilità esterna o interna, assenza per malattia o altra causa per periodi superiori ai sei mesi;
- cancellazione dell'account ove l'incaricato abbia perso le abilitazioni per il trattamenti dai dati.

D. Lgs. 196/03 - Art 34 Comma 1 lett e): protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentititi e a determinati programmi informatici.

Allegato B - Disciplinare Tecnico - Punto 9

Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Misura da adottare

La norma in oggetto demanda al Titolare il compito di individuare, predisporre e comunicare istruzioni scritte per gli incaricati del trattamento affinché, durante una sessione attiva di trattamento dei dati, lo strumento utilizzato non rimanga incustodito

Si tratta di una misura di sicurezza organizzativa rivolta alla protezione dei dati sia da eventuali manomissioni, sia dall'accesso agli stessi da parte di soggetti non autorizzati.

Sarà fatto obbligo, anche attraverso l'assistenza di un soggetto competente a tale scopo incaricato, che tutti i dipendenti dell'Ente provvedano a:

- attivare sulla propria postazione di lavoro un "salvaschermo" che entri in azione dopo tre minuti di inattività del computer;
- disattivare il collegamento alla rete di trasmissione dati quando non sia necessaria la connessione;
- spegnere il proprio elaboratore in caso di prolungata assenza dall'ufficio

---

D. Lgs. 196/03 - Art 34 . Comma 1 lett. e): protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentititi e a determinati programmi informatici

Allegato B - Disciplinare Tecnico - Punto 10

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali si può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per **esclusive necessità di operatività e di sicurezza del sistema**

In tal caso la custodia delle copie delle credenziali di autenticazione è organizzata garantendo la relativa segretezza e individuando, preventivamente per iscritto, i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato

Misura da adottare

Sarà fatto obbligo di adottare la seguente procedura operativa:

- l'incaricato del trattamento dei dati annotterà su un foglio da inserire in busta chiusa e da lui sigillata la parola chiave che verrà consegnata al proprio Responsabile di Area/Responsabile del Trattamento;
- la busta verrà aperta, come prescritto dalla norma, **qualora si verifichi una prolungata assenza dell'incaricato e solo ed esclusivamente per esigenze di operatività e di sicurezza del sistema;**
- all'atto del ritorno in attività, l'incaricato, provvederà alla modifica della parola chiave e

nuovamente alla sua annotazione su foglio secretato e consegnato in custodia al Responsabile di Area/Responsabile del Trattamento.

D. Lgs. 196/03 - Art 34 . Comma 1 lett. c): utilizzazione di un sistema di autorizzazione.

Allegato B - Disciplinare Tecnico - Punti 12,13,14,15

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Nell'ambito dell'aggiornamento periodico, con cadenza almeno annuale, dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, viene predisposta la lista degli incaricati redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Misura da adottare
La norma in esame disciplina l'ipotesi in cui agli stessi dati accedano più incaricati con profili di AUTORIZZAZIONE DIVERSI. Ad esempio, alcuni incaricati possono solo consultare i dati ma non modificarli mentre altri sono autorizzati al loro aggiornamento, rettifica o cancellazione.

L'Ente procederà secondo le seguenti indicazioni:

- sarà fatta almeno una volta all'anno una ricognizione per verificare i profili di incarico e saranno confermati o aggiornati i trattamenti e le operazioni consentiti ai singoli incaricati;
- in caso di perdita delle qualità legittimanti (mobilità, quiescenza ecc) di un incaricato, si provvederà a dare disposizioni per la cancellazione immediata dall'elenco degli incaricati ed all'adeguamento delle tabelle dei privilegi secondo le necessità.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

D. Lgs. 196/03 - Art 34 . Comma 1 lett. e): protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentititi e a determinati programmi informatici.

Allegato B - Disciplinare Tecnico - Punto 16

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Misura da adottare
Considerata la circostanza che i Virus attualmente più diffusi sono di tipo Internet Worm con funzionalità di mass mailing e che includono nel loro codice anche attacchi basati su specifiche vulnerabilità del sistema operativo o delle applicazioni, la prevenzione e gli obblighi di legge richiedono le seguenti misure tecniche ed organizzative:

- ❑ installare e aggiornare frequentemente programmi Anitivirus;
- ❑ installare periodicamente gli ultimi aggiornamenti (patch, service pack, hotfix) del sistema operativo e delle applicazioni;
- ❑ formare gli incaricati del trattamento su tali tipologie di rischio.

In particolare si provvederà affinché tutte le postazioni che trattano dati personali siano costantemente aggiornate con adeguato **software antivirus** da Sistema Centralizzato. Il software Antivirus deve possedere le seguenti caratteristiche minime:

- Residente In Memoria;
- Minidisco Emergenza;
- Aggiornamenti Tempestivi del Produttore;
- Scansione Allegati ed e-mail;
- Ricerca Virus nel Boot/Master e nel file di sistema in Tempo Reale;
- Aggiornamento da internet;
- Scansione Virus, Worm, Trojan e mal-ware in generale;
- Capacità isolamento file infetti;
- Help On line

Sulla base dell'analisi dei casi, degli incidenti, delle diverse tipologie di virus e worm circolanti, delle modalità con cui si propaga un'infezione all'interno di un contesto lavorativo, è possibile formulare un elenco di raccomandazioni utili per la prevenzione e la prtezione dei dati che saranno osservate all'interno dell'Ente:

- ❑ Consultare, esaminare e diffondere messaggi specializzati di virus alert;
- ❑ Nella posta elettronica, quando si introducono allegati, nel caso vengano inviati documenti scritti con MS Word, si usi il formato RTF e non quello .Doc;
- ❑ Configurare le schermate in modo che sia possibile visualizzare l'estensione dei files;
- ❑ Non aprire allegati che contengano un'estensione doppia;
- ❑ In caso di ricezione di una e-mail con oggetto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato;
- ❑ Non considerare le icone mostrate dagli allegati come garanzia dell'integrità del software;

- In caso di ricezione di e-mail non richieste o con contenuti insoliti, non eseguire senza aver preventivamente valutato la circostanza, collegamenti a indirizzi web presenti nel testo della e-mail;
- Controllare bene che i CD masterizzati e scambiati siano immuni da virus;
- Evitare di prelevare software da sorgenti poco affidabili.

D. Lgs. 196/03 - Art 34 . Comma 1 lett. e): protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentititi e a determinati programmi informatici

Allegato B - Disciplinare Tecnico - Punto 17

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti sono effettuati almeno annualmente. In caso di trattamenti di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

Misura da adottare
Il Software utilizzato contiene spesso difetti. La ricerca di tali difetti è costantemente fatta dagli stessi fornitori. Quando viene individuata una vulnerabilità, i fornitori rilasciano gratuitamente il software correttivo ma questo non sempre viene installato

L'Ente provvederà affinché venga periodicamente verificato lo stato di efficienza e di capacità di protezione dei sistemi hardware e del software di base sia relativamente ai server che alle singole postazioni di lavoro.

La verifica dovrà produrre un documento tecnico che dia indicazioni su quanto segue:
- evidenza dei sistemi hardware obsoleti e da dismettere;
- disponibilità di patch, fix, service pack e nuove versioni da fornire agli utenti, ove possibile tramite sistemi centralizzati di distribuzione

---

D. Lgs. 196/03 - Art 34 . Comma 1 lett. f): adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Allegato B - Disciplinare Tecnico - Punto 18

Sono impartite istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale.

Misura Da Adottare

La misura di sicurezza è finalizzata a garantire che i dati personali trattati siano sempre disponibili e integri Purtroppo non in tutte le Amministrazioni Pubbliche la cultura della produzione di copie di salvataggio dei dati appare diffusa.

In alcuni casi l'attività di salvataggio dei dati viene trascurata, non considerata o non fatta in maniera sistematica. Per questa ragione il Legislatore ha voluto tutelare l'integrità e la disponibilità dei dati con una prescrizione tecnico-organizzativa considerata di base nella cultura della sicurezza informatica.

La produzione sistematica di copie di sicurezza è un processo articolato e di complessa gestione che richiede tempo.

L'Ente, procederà ad adeguare la propria condotta ai dettami legislativi secondo le specifiche di seguito riportate:

- si individueranno specifiche procedure attraverso le quali sarà previsto l'obbligo tassativo di effettuazione delle copie di sicurezza nelle modalità ritenute opportune da ciascun Responsabile del Trattamento

In particolare, dovranno essere osservate le seguenti misure di prevenzione e protezione:

- effettuazione di copie giornaliere incrementali su supporti di buona qualità ed affidabilità. Potrà essere utilizzato qualsiasi tipo di supporto, magnetico, ottico, scrivibile o riscrivibile Nel caso di utilizzo di supporto riscrivibile, ottico o magnetico sarà opportuno verificare attentamente la correttezza della operazione di cancellazione del preesistente contenuto;
- effettuazione di copie di dati con cadenza almeno settimanale;
- custodia dei supporti di memoria utilizzati in locale idoneo e separato da quello in cui viene effettuato il trattamento dei dati in esercizio;
- conservazione "perenne", sino a diversa disposizione delle copie su base annuale;
- verifica almeno settimanale di correttezza delle copie effettuate

All'interno di ciascuna Area, sarà definita una procedura per quanto concerne:

- La periodicità delle frequenza e la modalità del salvataggio dei dati;
- La tipologia dei supporti da utilizzare per le copie di backup e il numero di copie da effettuare;
- I criteri da utilizzare per le verifica della correttezza delle copie effettuate.

Ad ogni incaricato sarà fatto obbligo di effettuare con periodicità definita, le copie di backup.

Dati Sensibili e Giudiziari

D. Lgs. 196/03 - Art 34 . Comma 1 lett. e): protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentititi e a determinati programmi informatici

Allegato B - Disciplinare Tecnico - Punto 20

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici

Misura da adottare

Gli accessi abusivi comportano tutta una serie di rischi di natura tecnica, operativa e legale.
Più analiticamente i rischi riguardano:

- Conoscenza dei dati da parte di persone non autorizzate;
- Distruzione o perdita totale o parziale dei dati;
- Danneggiamento dei dati;
- Diffusione di documenti, anche riservati;
- Impossibilità di svolgere operazioni di trattamento dei dati;
- Diffusione di programmi informatici infetti;
- Rallentamento delle capacità del sistema;
- Perdita di tempo.

Tra le principali circostanze che favoriscono gli accessi abusivi alcune sono ricorrenti e riguardano:

1) Account senza Password o con Password deboli. Tutti i sistemi protetti da parole chiave deboli o addirittura predefinite sono facilmente attaccabili
2) Numero elevato di porte aperte I sistemi telematici funzionano e comunicano tra loro attraverso canali di comunicazione che, all'ingresso nel domicilio informatico del proprio sistema assumono il nome di Porta. Le porte sono tante e hanno diverse e precise funzioni. Molto spesso, queste porte sono lasciate attive, cioè aperte, anche quando non sono necessarie per motivi di lavoro. Le porte lasciate aperte, costituiscono una delle maggiori criticità per la vulnerabilità del sistema.

In aggiunta alle prescrizioni già previste per i dati personali, all'interno di ciascuna Area, nel caso di trattamento di dati Sensibili e/o Giudiziari, sarà preteso il rigoroso rispetto delle seguenti prescrizioni:

- divieto assoluto di utilizzare codici identificativi senza parole chiave o con parole chiave "deboli" che non seguano le prescrizioni contenute nella Regola 5 dell'Allegato B al D. Lgs. 196/03;
- obbligo di "chiudere" tutte le porte logiche di accesso non utilizzate sulle unità di elaborazione di tipo server e sulle singole postazioni di lavoro agendo sul sistema operativo o su eventuali software di corredo (firewall personali).

A livello più generale si imporrà:

- l'obbligo di monitorare continuamente l'efficienza della protezione delle Rete Locale dell'Ente assicurata dal Firewall al fine di controllare e filtrare il traffico in entrata e quindi ridurre fisiologicamente il rischio di accessi abusivi

---

D. Lgs. 196/03 - Art 34 . Comma 1 lett. f): adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi

Allegato B - Disciplinare Tecnico - Punto 21

Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti

Misura da adottare

Dovranno essere adottate procedure formali affinché:

- le copie di sicurezza dei dati siano conservate in luogo fisico diverso da quello in cui è ubicata l'unità di elaborazione utilizzata per il trattamento;
- le copie di sicurezza siano conservate in luoghi protetti da fonti di calore, campi magnetici, interferenze elettromagnetiche , intrusioni, incendi ed allagamenti;
- l'accesso ai locali contenenti le copie sia limitato ai Responsabili, agli Incaricati o all'Amministratore di Sistema Informatico se individuato.

D. Lgs. 196/03 - Art 34 . Comma 1 lett. f): adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Allegato B - Disciplinare Tecnico - Punto 22

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono eventualmente essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, solo ove le informazioni precedentemente in essi contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili.

Misura da adottare

- Sarà fatto obbligo a tutto il personale di effettuare la cancellazione dei supporti non più utilizzati attraverso procedure che assicurino la completa cancellazione dei dati in essi contenuti, suggerendo comunque la **distruzione dei supporti nei casi di mancanza di tali garanzie**.

D. Lgs. 196/03 - Art 34 . Comma 1 lett. f): adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Allegato B - Disciplinare Tecnico - Punto 23

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Misura da adottare

- All'interno di ciascuna Area si provvederà affinché per i sistemi che contengono dati sensibili o giudiziari (per i quali è previsto un tempo certo di ripristino compatibile con i diritti degli interessati non superiore a sette giorni) sia previsto un sistema hardware di emergenza (backup)

che possa garantire le condizioni minime essenziali di funzionamento dello stesso, sino al ripristino del sistema principale, previa regolare effettuazione delle copie di backup dei dati e del sistema operativo unitamente ad una procedura formalizzata che descriva in modo chiaro ruoli, compiti e scadenze, tempi e modalità di ripristino;

- Si provvederà a correggere eventuali bugs (errori) del sistema operativo e degli applicativi.

Allegato B - Disciplinare Tecnico - Punti 25 e 26

Nel caso in cui il Titolare adotti misure minime di sicurezza avvalendosi di soggetti esterni alla struttura, per provvedere alla esecuzione riceverà dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la **conformità alle disposizioni del presente disciplinare tecnico**.

Misura da adottare

- Si provvederà affinché, in occasione di ogni intervento sul sistema informativo, sull' hardware o sul software da parte di soggetti esterni all'Ente, sia redatta da parte degli stessi una dichiarazione scritta che ne attesti la regolare esecuzione in conformità alle disposizioni della Codice ed in particolare del Disciplinare Tecnico.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 6.2 Misure di sicurezza Idonee Art. 31 D. Lgs. 196/03

Misure di Sicurezza Idonee (art. 31 D. Lgs. 196/03)

La disciplina in materia di protezione dei dati personali impone al Titolare di adottare, oltre alle misure minime espressamente previste, "idonee e preventive misure di sicurezza" che dovranno tener conto dei seguenti fattori:

- delle conoscenze acquisite in base al progresso tecnico;
- della natura dei dati oggetto del trattamento;
- delle specifiche caratteristiche del trattamento, ossia se esso venga eseguito con l'ausilio di mezzi elettronici o meno

Si osserva, il richiamo esplicito del testo di legge al PROGRESSO TECNICO, che consente una "forbice" interpretativa particolarmente ampia all'interno della quale far rientrare le varie e possibili misure di sicurezza
Ciò spiega il percorso seguito dal Legislatore che ha portato all'adozione di due diversi regimi di responsabilità nel caso di violazione di misure minime o di misure idonee, assegnando alle prime una rilevanza penale e, alle seconde, una rilevanza essenzialmente civile, con valutazioni da compiere al verificarsi del caso concreto e tenuto conto dello stadio di progresso tecnologicamente raggiunto e delle soluzioni concretamente disponibili sul mercato.

Il risultato del citato percorso seguito dal Legislatore comporta che, le misure idonee non sono identificate dalla norma ma devono essere sempre aggiornate alle nuove scoperte della tecnologia, mentre, per le misure minime si è prevista la necessità della puntuale identificazione da parte del legislatore.

L'Analisi dei Rischi esplicitata nella Sezione 5 e nella Sezione 5.1, ha consentito di rilevare le Minacce Reali ed il Rischio Residuo che insiste, in senso generalizzato e trasversale, su tutte le Aree/Settori dell'Ente senza distinzione e, di conseguenza, sui dati di ogni specifica Banca Dati censita

Il Rischio Residuo risultante deve essere abbattuto o quantomeno ridotto (ex Art. 31 D. Lgs. 196/03) al fine di evitare che i dati possano andare incontro ai seguenti eventi dannosi:

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

EVENTO DANNOSO	QUALITA' A RISCHIO DI PERDITA		
	DISPONIBILITA'	INTEGRITA'	RISERVATEZZA
FURTO ARCHIVI CARTACEI	✔		✔
EVENTO DISTRUTTIVO VOLONTARIO	✔	✔	
DANNEGGIAMENTO DOCUMENTI CARTACEI	✔	✔	
INAGIBILITA' DEI LOCALI		✔	
FURTO HARDWARE	✔		✔
FURTO SUPPORTI MEMORIA	✔		✔
GUASTO TECNICO HARDWARE	✔	✔	
DETERIORAMENTO SUPPORTI MEMORIA	✔	✔	
SABOTTAGGIO HARDWARE	✔	✔	
INTASAMENTO POSTA ELETTRONICA	✔		
ERRORI DI TRASMISSIONE DATI		✔	
SABOTTAGGIO RETI DI TRASMISSIONE	✔	✔	
INTERCERCETTAZIONE TRAFFICO IN RETE DATI			✔
LETTURA, COPIA E MANOMISSIONE BANCHE DATI RISERVATE	✔	✔	✔
PERDITA E/O DANNEGGIAMENTO BANCHE DATI RISERVATE	✔	✔	✔
GESTIONE SICUREZZA ERRATTA	✔	✔	✔
COMPORTAMENTO NEGLIGENTE E COLPEVOLE	✔	✔	✔
FURTO CREDENZIALI AUTORIZZAZIONE	✔	✔	✔

A fronte degli Eventi Dannosi che possono essere prodotti sui dati trattati dalle Minacce Reali e dei Rischi Residui risultanti dalla Valutazione operata, in questa sottosezione del documento sono riportate le **Misure di Sicurezza Idonee** che l'Ente si impegna ad applicare.

Tali Misure saranno applicate compatibilmente con i vincoli ed i limiti derivanti dalle esistenti infrastrutture edili e tecnologiche, dalle disponibilità finanziarie e dal Piano delle Assunzioni del Personale e, in armonia, con il piano di realizzazione degli interventi strutturali riconducibili ad altre iniziative specifiche

In senso generale si provvederà a sensibilizzare l'Amministrazione sulla problematica relativa alla Sicurezza nel trattamento dei Dati Personali, Sensibili e Giudiziari realizzando una serie di interventi (rivolti a ridurre il Rischio Residuo derivante dalle minacce rilevate) di tipo:

- Infrastrutturale;
- Procedurale;
- Tecnico-Informatico;

Legenda Rischio Residuo (RR) (con il significato assunto in Sezione 5, Sezione 5.1 e nell'Allegato 3)

Il Rischio Residuo è stato valutato in termini di:

✓ accettabilità;

⊘ non accettabilità

con il seguente significato:

✓ accettabilità

riferita sia a basse probabilità di accadimento della minaccia-evento dannoso, che a contenute vulnerabilità di contesto.

⊘ non accettabilità

riferita sia a medio-alte probabilità di accadimento della minaccia-evento dannoso che ad un livello medio-alto di vulnerabilità di contesto.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

INFRASTRUTTURE

EVENTO DANNOSO	RR	MISURA IDONEA DA ADOTTARE
1. Furto archivi cartacei	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato nelle ore d'ufficio e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale ■ Tutti i documenti contenenti dati personali sensibili e giudiziari, devono essere custoditi in armadi e cassetti chiusi a chiave. ■ Fuori dagli orari di lavoro nessun tipo di documento deve essere lasciato incustodito. ■ Le chiavi degli armadi non devono essere universali. In caso di prolungata assenza del personale e fuori dagli orari di lavoro le chiavi non devono essere lasciate all'interno dell'ufficio ma dovranno essere custodite da ogni singolo incaricato del trattamento con copia presso ciascun responsabile in busta chiusa e sigillata. ■ I documenti idonei a rivelare lo stato di salute e la vita sessuale devono essere conservati separatamente da ogni altro dato la cui finalità non richiede il loro utilizzo. Dove ciò non fosse possibile gli stessi documenti dovranno essere conservati in sezioni o sottofascicoli da conservare chiusi o con modalità tali da ridurre la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative. ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni. ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti. ■ Si provvederà alla installazione ed al potenziamento di sistemi antintrusione dell'Ente; ■ Si provvederà a dotare tutto il personale dell'Ente di un cartellino di identificazione ai sensi delle vigenti leggi. ■ Gli archivi storici saranno dotati di idonee protezioni antintrusione antincendio e di adeguato impianto di climatizzazione. L'accesso deve essere controllato. Per accedere a tale archivio le persone devono essere preventivamente autorizzate e nel caso in cui l'accesso avvenga dopo l'orario di chiusura devono essere identificate e registrate

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

2. **Evento distruttivo volontario**	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato nelle ore d'ufficio e chiusi a chiave in caso di prolungata assenza del personale La chiave deve essere diversa per ogni locale. ■ Tutti i documenti contenenti dati personali sensibili e giudiziari, devono essere custoditi in armadi e cassetti chiusi a chiave. ■ Fuori dagli orari di lavoro nessun tipo di documento deve essere lasciato incustodito. ■ Si provvederà alla installazione ed al potenziamento di sistemi antintrusione dell'Ente; ■ Le chiavi degli armadi non devono essere universali. In caso di prolungata assenza del personale e fuori dagli orari di lavoro non devono essere lasciate nel rispettivo ufficio e dovranno essere custodite da ogni singolo incaricato del trattamento con copia presso ciascun responsabile in busta chiusa e sigillata. ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni; ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti; ■ Si provvederà a dotare tutto il personale dell'Ente di un cartellino di identificazione ai sensi delle vigenti normative; ■ L'accesso all'archivio storico deve essere controllato. Per accedere a tale archivio le persone devono essere preventivamente autorizzate e nel caso in cui l'accesso avvenga dopo l'orario di chiusura devono essere identificate e registrate.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

3. **Danneggiamento documenti cartacei**	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato nelle ore d'ufficio e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale. ■ Tutti i documenti contenenti dati personali sensibili e giudiziari devono essere custoditi in armadi e cassetti chiusi a chiave. ■ Fuori dagli orari di lavoro nessun tipo di documento deve essere lasciato incustodito. ■ Le chiavi degli armadi non devono essere universali. In caso di prolungata assenza del personale e fuori dagli orari di lavoro non devono essere lasciate nel rispettivo ufficio e dovranno essere custodite da ogni singolo incaricato del trattamento con copia presso ciascun responsabile in busta chiusa e sigillata. ■ Si provvederà alla installazione ed al potenziamento di sistemi antintrusione dell'Ente; ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni; ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti; ■ Si provvederà a dotare tutto il personale degli uffici di un cartellino di identificazione ai sensi delle vigenti leggi. **Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>incendio</u> saranno adottate le seguenti misure:** ■ Saranno verificati e resi pienamente efficienti tutti i dispositivi antincendio presenti negli ambienti in cui sono effettuati trattamenti di dati personali. ■ Se valutato necessario sarà incrementato il numero degli estintori a polvere e a CO_2. ■ Saranno emanate specifiche informazioni e raccomandazioni ed avvisi in armonia con quanto già previsto dalla vigente normativa in tema di Sicurezza sul Lavoro (D. Lgs. 626/94).

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

4	Inagibilità Locali	⊘	Per contrastare il rischio residuo derivante dal verificarsi della minaccia di incendio saranno adottate le seguenti misure: ■ Saranno verificati e resi pienamente efficienti tutti i dispositivi antincendio presenti negli ambienti in cui sono effettuati trattamenti di dati personali. ■ Se valutato necessario sarà incrementato il numero degli estintori a polvere ed a CO_2. ■ Saranno emanate specifiche informazioni e raccomandazioni ed avvisi in armonia con quanto già previsto dalla vigente normativa in tema di Sicurezza sul Lavoro (D. Lgs. 626/94).

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

STRUMENTI ELETTRONICI

EVENTO DANNOSO	RR	MISURA IDONEA DA ADOTTARE
5. Furto Hardware	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato nelle ore d'ufficio e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale ■ Si provvederà alla installazione ed al potenziamento di sistemi antintrusione dell'Ente; ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni; ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti; ■ Si provvederà a dotare tutto il personale degli uffici di un cartellino di identificazione ai sensi delle vigenti leggi.
6. Furto Supporti Memoria	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ Saranno emanate procedure formali per l'accesso controllato e regolamentato nei locali ove ha luogo la custodia dei supporti magnetici o ottici. ■ Sarà verificato periodicamente il rispetto delle procedure di cui sopra.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

7.	**Guasto Hardware**	**Tecnico**	**Per contrastare il rischio residuo derivante dal verificarsi di tale minaccia – evento dannoso saranno adottate le seguenti misure:** ■ Tutte le Unità di Elaborazione saranno acquistate o noleggiate con un periodo di garanzia on site pari almeno a tre anni; ■ Si provvederà a censire e catalogare tutte le Unità di Elaborazione dell'Ente al fine di disporre di un quadro sempre aggiornato del livello di obsolescenza tecnica e degli interventi tecnici effettuati sulle macchine; ■ Si procederà con gradualità alla dismissione dell' hardware tecnologicamente obsoleto; ■ Si provvederà ad adottare una politica di acquisto delle Unità di Elaborazione di tipo Server con caratteristiche di ridondanza nei dischi (Mirroring o RAID) negli alimentatori elettrici e nelle schede di rete **Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>incendio</u> saranno adottate le seguenti misure:** ■ Saranno verificati e resi pienamente efficienti tutti i dispositivi antincendio presenti negli ambienti in cui sono effettuati trattamenti di dati personali. ■ Se valutato necessario sarà incrementato il numero degli estintori a polvere ed a CO_2. ■ Saranno emanate specifiche informazioni e raccomandazioni ed avvisi in armonia con quanto già previsto dalla vigente normativa in tema di Sicurezza sul Lavoro (D. Lgs. 626/94)

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

8	**Deterioramento Supporti Memoria**	⊘	**Per contrastare il rischio residuo derivante da tale evento dannoso saranno adottate le seguenti misure:** ■ Si provvederà all'acquisizione di supporti magnetici o ottici per la memorizzazione dei dati (CDR, CDRW, DVD, nastri, floppy) con caratteristiche di alta affidabilità; ■ Si provvederà alla custodia delle copie di backup (in numero adeguato alle necessità) in luogo adeguato, sufficientemente distante dall' ambiente in cui vengono trattati i dati e protetto da agenti ambientali (tale da non risentire delle conseguenze delle minacce di un eventuale evento distruttivo o corruttivo dei sistemi hardware); ■ Si provvederà alla custodia delle copie dei dati sensibili e giudiziari in armadi o contenitori muniti di serratura; **Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>incendio</u> saranno adottate le seguenti misure:** ■ Saranno verificati e resi pienamente efficienti tutti i dispositivi antincendio presenti negli ambienti in cui sono effettuati trattamenti di dati personali. ■ Se valutato necessario sarà incrementato il numero degli estintori a polvere ed a CO_2 ■ Saranno emanate specifiche informazioni e raccomandazioni ed avvisi in armonia con quanto già previsto dalla vigente normativa in tema di Sicurezza sul Lavoro (D. Lgs 626/94).
9	**Sabottaggio Hardware**	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale. ■ Si provvederà alla installazione ed al potenziamento di sistemi antintrusione dell'Ente; ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni; ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti; ■ Si provvederà a dotare tutto il personale degli uffici di un cartellino di identificazione ai sensi delle vigenti leggi.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C S € 90.000,00 (i.v.)
REA 228746

10	Intasamento Posta elettronica	⊘	**Per contrastare il rischio residuo derivante dal verificarsi dalla minaccia di spamming saranno adottate le seguenti misure:** ■ Saranno emanate specifiche regole di comportamento verso tutto il personale al fine di renderlo edotto sull'uso consapevole e corretto della Posta Elettronica e dei Servizi Internet; ■ Saranno utilizzate solo e-mail istituzionali con efficace servizio anti-spamming; ■ Sarà attuato un programma di graduale diffusione della Posta Elettronica Certificata secondo le raccomandazioni dei programmi ministeriali/AIPA/CNIPA;
11	Errori di trasmissione in rete dati	⊘	**Per contrastare il rischio residuo derivante dal verificarsi dalla minaccia di traffico anomalo saranno adottate le seguenti misure:** ■ Sarà rafforzato l'esercizio di efficaci strumenti di controllo del traffico in rete tesi ad evidenziare il traffico anomalo e far sì che in ogni rete interconnessa vengano rispettati i relativi requisiti di sicurezza definiti dalle specifiche politiche, al fine di non creare danni o disservizi; ■ Saranno emanate specifiche regole di comportamento verso tutto il personale al fine di renderlo edotto sull'uso consapevole e corretto della Rete Locale ed Internet.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

12 Sabotaggio Rete	⊘	**Per contrastare il rischio residuo derivante dal verificarsi di tale evento dannoso sarà adottata le seguenti misura:** ■ I cablaggi della rete locale saranno mantenuti in cabalette sigillate o protette, possibilmente, sottotraccia **Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>accesso non autorizzato all'infrastruttura</u> saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale ■ Saranno mantenuti in piena efficienza e se possibile potenziati, in tutti gli uffici, i sistemi di antintrusione soprattutto in quelli collocati al Piano Terra più agevolmente raggiungibili dall'esterno; ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni; ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti; ■ Si provvederà a dotare tutto il personale di un cartellino di identificazione ai sensi delle vigenti leggi.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

13. Intercettazione traffico di rete	⊘	**Per contrastare il rischio residuo derivante dal verificarsi delle minacce di <u>accesso non autorizzato ad archivi informatici</u> e <u>impersonamento in un altro soggetto</u> saranno adottate le seguenti misure:** ■ Saranno mantenuti efficaci sistemi di identificazione ed autenticazione dell'utente in rete; ■ Saranno mantenuti efficaci sistemi software di controllo delle Intrusioni in rete; ■ Sarà promosso, al fine di ridurre il Rischio Residuo derivante dal verificarsi di tali minaccia, l'utilizzo della crittografia ed in particolare della Firma Digitale, con l'obiettivo di realizzare la sicurezza dei servizi di rete attraverso una infrastruttura tecnologica di crittografia a Chiave Pubblica (PKI).
14. Lettura, copia e manomissioni banche dati riservate	⊘	**Per contrastare il rischio residuo derivante dalla minaccia di <u>accesso non autorizzato agli archivi informatici</u> saranno adottate le seguenti misure:** ■ Saranno rafforzate e sottoposte a periodica revisione le misure di identificazione ed autenticazione dell'utente in rete LAN da parte dei Server Gestionali affinché in ogni rete interconnessa vengano rispettati i relativi requisiti di sicurezza definiti dalle specifiche politiche; ■ Saranno sottoposte a periodica revisione le regole di apertura delle porte necessarie per i servizi pubblici in produzione (tipicamente server web, server di posta, DNS, FTP); ■ L'Ente si doterà di un firewall perimetrale ■ Tutte le stazioni di lavoro sulle quali vengono effettuati trattamenti di dati personali saranno protette a monte da un sistema di Protezione Personale contro le Intrusioni (Firewall Personale) ■ Sarà sottoposto a periodico monitoraggio il funzionamento del Firewall effettuando periodici test di simulazione di intrusione. **Per contrastare il rischio residuo derivante dal verificarsi delle minacce di <u>impersonamento in un altro soggetto</u> saranno adottate le seguenti misure:** ■ Saranno mantenuti efficaci sistemi di identificazione ed autenticazione dell'utente in rete; ■ Saranno mantenuti efficaci sistemi software di controllo delle Intrusioni in rete; ■ Sarà promosso, al fine di ridurre il RR derivante dal verificarsi di tali minaccia, l'utilizzo della crittografia ed in particolare della Firma Digitale, con l'obiettivo di realizzare la sicurezza dei servizi di rete attraverso una infrastruttura tecnologica di crittografia a Chiave Pubblica (PKI)

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 -- 09128 Cagliari
Tel 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

15. Perdita e/o danneggiamento banche dati	⊘	**Per contrastare il rischio residuo derivante dal verificarsi dalla minaccia di codice software difettoso saranno adottate le seguenti misure:** ■ Si procederà ad una progressiva omogeneizzazione delle versioni dei sistemi operativi delle unità di elaborazione alle ultime versioni in commercio (Windows, Linux o altri sistemi operativi, Ms-Office, privilegiando i programmi OPEN SOURCE ed applicando la norma sul riuso del software in P.A.); ■ Saranno emanate Regole di Comportamenti rivolte a tutto il personale specificanti l'obbligo di utilizzare solo ed esclusivamente software con regolari diritti di proprietà da parte dell'Ente; ■ Sarà realizzato e mantenuto sempre aggiornato un inventario delle risorse software dell'Ente, preferibilmente utilizzando sistemi, economici e di facile utilizzo da parte di tutto il personale. **Per contrastare il rischio residuo derivante dal verificarsi dalla minaccia di codice software maligno saranno adottate le seguenti misure:** ■ Si provvederà a mantenere in piena efficienza i Software Antivirus. L'automatismo e la tempestività degli aggiornamenti disponibili per tutto il personale elimineranno in modo significativo i rischi derivanti da tale minaccia. ■ L'Ente si doterà di un server antivirus da sistema Centralizzato in modo da provvedere in tempo reale alla distribuzione del software e degli aggiornamenti agli utenti collegati in rete. **Per contrastare il rischio residuo derivante dal verificarsi della minaccia di accesso non autorizzato all'infrastruttura saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato e chiusi a chiave in caso di prolungata assenza del personale La chiave deve essere diversa per ogni locale ■ Saranno mantenuti in piena efficienza e se possibile potenziati, in tutti gli uffici, i sistemi di antintrusione soprattutto in quelli collocati al Piano Terra più agevolmente raggiungibili dall'esterno; ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni; ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti; ■ Si provvederà a dotare tutto il personale degli uffici di un cartellino di identificazione ai sensi delle vigenti leggi. **Per contrastare il rischio residuo derivante dal verificarsi della minaccia di incendio saranno adottate le seguenti misure:** ■ Saranno verificati e resi pienamente efficienti tutti i dispositivi antincendio presenti negli ambienti in cui sono effettuati trattamenti di dati personali ■ Se valutato necessario sarà incrementato il numero degli estintori a polvere ed a CO_2 ■ Saranno emanate specifiche informazioni e raccomandazioni ed avvisi in armonia con quanto già previsto dalla vigente normativa in tema di Sicurezza sul Lavoro (D. Lgs. 626/94).

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

ORGANIZZAZIONE

MINACCIA REALE	RR	MISURA IDONEA DA ADOTTARE
16 Gestione Sicurezza errata	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di comportamento errato saranno adottate le seguenti misure:** ■ Sarà curata la formazione "continua" dei Responsabili e degli incaricati in tema di Sicurezza nel trattamento dei Dati ed in particolare sulla corretta gestione delle Unità di Elaborazione in armonia con quanto previsto nelle Sezione 9 del presente documento; ■ Saranno impartite, chiare istruzioni scritte riguardanti i compiti assegnati agi incaricati in tutte le fasi di trattamento dei dati personali e ove necessario saranno apposti avvisi in bacheca
17 Comportamento Negligente e colpevole	⊘	**Per contrastare il rischio residuo derivante dal verificarsi di tale evento dannoso saranno adottate le seguenti misure:** ■ Sarà affettata una rilevazione puntuale delle reali esigenze informative di accesso alla Rete Internet da parte del personale interno, al fine di ridurre gli accessi generalizzati alla Rete e di conseguenza la possibilità di contrarre virus informatici; ■ Sarà confermato il divieto di utilizzo di caselle di posta personali ed obbligo di utilizzo di caselle di posta istituzionale dotate di servizio antispamming, antivirus, meglio se certificate
18 Furto Credenziali	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di accesso non autorizzato saranno adottate le seguenti misure:** ■ Sarà curata la formazione continua degli Incaricati sul tema specifico della custodia e buon uso delle credenziali ■ Saranno emanate specifiche norme volte a sensibilizzare gli incaricati sull'uso corretto delle credenziali e sulle sanzioni per l'Ente in caso di omissione di tale adempimento

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 7 Descrizione dei Criteri e delle Modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (Regola 19.5 e Regola 23 Allegato B al D. Lgs. 196/03)

Disciplinare Tecnico – Allegato B al D. Lgs. 196/03

Regola 19.5. Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

Regola 23 Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Nella presente sezione sono descritti i criteri e le modalità per il ripristino della disponibilità dei dati sensibili o giudiziari in seguito a distruzione o danneggiamento degli stessi o degli strumenti elettronici sui quali sono conservati, secondo quanto prescritto dalla Regola 23.

Il **ripristino** o Disaster Recovery è quel processo che consente di ripristinare il normale o indispensabile funzionamento dell'operatività del sistema e il trattamento dei dati interrotti da un evento indesiderato di natura eccezionale.

Il piano di Disaster Recovery definisce perciò le procedure tecniche e organizzative alternative e sostitutive rispetto a quelle normalmente in uso, per fronteggiare un evento catastrofico che renda indisponibili le risorse dell'Ente deputate alle operazioni di elaborazione e trattamento dei dati

L'attività pratica di ripristino della disponibilità dei dati consiste nell'eseguire una nuova installazione di tutti i file di dati, dei programmi, del software di base che l'evento indesiderato ha alterato o distrutto, ovvero nella sostituzione delle componenti tecnologiche hardware che hanno provocato l'interruzione dei trattamenti. La nuova installazione avviene utilizzando le più aggiornate copie di sicurezza fatte su supporti o sistemi di riserva, accertandone preventivamente l'integrità.

La previsione da parte del Legislatore dell'obbligo di "istruzioni organizzative e tecniche" che prescrivano il salvataggio dei dati con una cadenza almeno settimanale mira a fare in modo che, in caso di "disastri informatici" non venga meno uno degli obiettivi principali della sicurezza nel trattamento dei dati: la disponibilità dei dati stessi

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

In considerazione della capienza dei moderni supporti di memorizzazione, la cadenza settimanale del backup dei dati si configura come una misura letteralmente MINIMA (Regola 18 Allegato B al D. Lgs. 196/03) e sarebbe opportuno orientare gli Uffici dell'Ente verso una procedura di backup dei dati automatizzata a cadenza giornaliera.

Il Programma delle Azioni, **al quale si conformano tutte le Aree dell'Ente che trattano dati di natura sensibile e giudiziaria**, atto ad assicurare il ripristino dei Sistemi, assumerà il nome di **Piano di Continuità Operativa**.

Esso sarà composto da due categorie di azioni:

- ⇨ Azioni o Misure Preventive
- ⇨ Azioni di Ripristino

Piano di Continuità Operativa - Misure Preventive

1. Saranno osservate tutte le prescrizioni normative in ordine all'ambiente fisico, all' hardware ed al software su cui risiedono i dati secondo le prescrizioni contenute nella Sezione 6 - Misure Minime di Sicurezza e Misure Idonee di Sicurezza ;

2. Saranno effettuate con regolarità le copie di sicurezza dei dati secondo le prescrizioni specificate dalla Regola 18 del Disciplinare Tecnico e nella Sezione 6 rif. Regola 18 del presente Documento;

3. Per tutte le Aree, all'interno delle quali vengono effettuati trattamenti di dati sensibili/giudiziari, sarà messa a disposizione un'unità di elaborazione di "backup" dotata di tutti gli strumenti elettronici necessari per la ripresa dei trattamenti interrotti nelle modalità richieste dalla legge, previa importazione dei dati di backup;

4. Sarà cura degli incaricati allo scopo nominati tenere traccia, con diligente cura, delle operazioni di trattamento effettuate sui dati al fine di consentire una più agevole ricostruzione dei dati in fase di ripristino;

5. Saranno impartite idonee istruzioni agli incaricati affinché rispettino le citate prescrizioni ed eseguano i compiti assegnati in modo corretto e conforme alla norma segnalando eventuali pericoli in modo tempestivo e chiaro al fine di consentire un efficace e rapido intervento da parte dei responsabili;

6. Saranno effettuate test reali di ripristino dei dati almeno una volta ogni sei mesi, utilizzando i sistemi sopra descritti

Piano di Continuità Operativa - Azioni di Ripristino

L'azione di ripristino ha l'obiettivo di restituire piena funzionalità ed efficienza al servizio di accesso ai dati interrotto e rendere quindi minime le perdite causate dall'interruzione dell'attività.

Per il Ripristino, una volta che siano state eseguite le azioni preventive in modo corretto, si opererà come segue:

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

1 a partire dal fermo della unità di elaborazione e dalla conseguente impossibilità di proseguire per un tempo non determinabile, si darà avvio al **Piano di Continuità Operativa;**

2 si provvederà, in primo luogo, in caso di interruzione dell'accesso ai dati che possa creare un disservizio al pubblico, a fornire tempestiva informazione, tramite avviso in Albo Pretorio, notizia sul Sito Internet e, se valutato necessario, attraverso gli organi di informazione;

3 si provvederà quindi a mettere in essere tutte le azioni necessarie per assicurare il ripristino della unità di elaborazione principale di esercizio (tramite assistenza tecnica interna e delle Ditte specializzate);

4 in parallelo a tale attività saranno recuperati dagli appositi armadi o contenitori, i supporti utilizzati per le ultime copie di backup effettuate;

5 sarà recuperata e verificata ogni eventuale documentazione cartacea utile a ricostruire con correttezza la situazione più aggiornata possibile prima dell'evento che ha determinato il fermo del sistema;

6 sarà attivato e reso pienamente funzionante il sistema di backup, preventivamente predisposto.

7 si provvederà ad effettuare, nel sistema di back up, il recovery della ultima copia dei dati e delle transazioni del giorno sino al perfetto allineamento dei due sistemi. Se necessario sarà preventivamente installato il software operativo ed applicativo necessario per il buon funzionamento dei programmi di trattamento dei dati;

8 si testerà la corretta esecuzione della procedura di ripristino dei dati nel sistema di backup e se positivo si restituirà il servizio interrotto al pubblico. Non sarà indispensabile in questo frangente disporre di tutte le funzionalità ma solo di quelle minime indispensabili per assicurare la ripresa delle attività al pubblico;

9 si opererà sul sistema di backup applicando le stesse regole e misure di sicurezza del sistema principale di esercizio ed inoltre si provvederà al ripristino del funzionamento del sistema principale di esercizio: si procederà in senso inverso a quanto eseguito, con un recovery delle copie di dati dal sistema di backup a quello di esercizio

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Di seguito si riporta una tabella sintetica riepilogativa delle procedure adottate dall'Ente per il salvataggio dei dati.

CRITERI E PROCEDURE PER IL SALVATAGGIO DEI DATI DA PARTE DELL'ENTE

CRITERI E PROCEDURE PER IL SALVATAGGIO	LUOGO DI CUSTODIA DELLE COPIE DI BACK UP	STRUTTURA DI RIFERIMENTO	PERIODICITA' DEL BACK UP
Ciascun Ufficio dell'Ente procede autonomamente alla effettuazione di copie di back up dei dati contenuti sui singoli Client, secondo le proprie esigenze, in modo del tutto autonomo, non regolamentato e con periodicità non espressamente definita (seppure almeno mensile). I supporti di memoria utilizzati per i salvataggi sono costituiti da CD, floppy disk ovvero DVD. **In particolare, l'Ufficio Ragioneria procede mensilmente ad effettuare le copie di sicurezza dei dati ospitati sull'elaboratore, utilizzando dei floppy disk come supporti di memoria che poi vengono custoditi all'interno di un cassetto dotato di serratura.** **L'Ufficio Servizi Sociali provvede mensilmente ad effettuare il backup dei**	I supporti di memoria utilizzati per il back up vengono conservati in armadi o cassetti muniti di serratura a cura di ciascun ufficio procedente.	CASA COMUNALE	**Il back up è effettuato secondo le esigenze proprie di ciascun Ufficio/Servizio in assenza di qualsivoglia regolamentazione in materia.** **In ogni caso, le copie di sicurezza vengono effettuate almeno una volta al mese.**

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

dati su CD successivamente custoditi in supporti muniti di serratura.. Anche i Servizi demografici, la Polizia Municipale, l'Ufficio Economato, l'Ufficio del Messo comunale, i Tributi, il Commercio ed il Protocollo procedono con cadenza mensile a realizzare le copie di sicurezza dei dati su CD che vengono custoditi all'interno di un cassetto munito di serratura.			

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 8 Previsione di interventi formativi

Disciplinare Tecnico

Regola 19.6 Previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

Il Titolare del trattamento dei dati deve, per legge, prevedere interventi formativi tesi a rendere formati e consapevoli gli incaricati del trattamento su quanto viene disposto dalla legge in materia di protezione dei dati personali, nonché su quanto sia contenuto nel D.P.S

Questo significa che l'incaricato deve conoscere non solo quanto prescritto dalla norma ma anche quanto predisposto dal titolare per la gestione dei dati e dei trattamenti all'interno dell'Ente

L'utilizzo da parte del Legislatore della parola "previsione" si deve interpretare nel senso che non è sufficiente che la formazione avvenga *una tantum*, ma è necessario che sia continua, ogniqualvolta avvengano cambiamenti di mansione degli incaricati, vengano introdotti nuovi strumenti o modalità con cui i dati sono trattati, oppure vi sia il rischio che si verifichino gravi problemi in ordine alla sicurezza.

L'Ente è consapevole che l'adeguamento alla norma, avrà un impatto considerevole sulla propria organizzazione interna.

Nel corso delle precedenti annualità l'Ente ha realizzato percorsi formativi specialistici in materia di riservatezza nel trattamento dei dati personali rivolti a tutti i soggetti che a qualsiasi titolo trattino dati personali nell'ambito dell'Amministrazione.

Per il futuro l'Ente ha elaborato un programma formativo finalizzato a perseguire i seguenti obiettivi principali:

- consentire il raggiungimento dell'adeguamento alla norma da parte dell'Ente rendendo i discenti edotti sui rischi che incombono sui dati e sulle misure di prevenzione e protezione disponibili per prevenire eventi dannosi;
- informare gli operatori in relazione ai profili di responsabilità personale e patrimoniale previsti dalla vigente normativa in materia;
- analizzare la problematica del contemperamento tra tutela del diritto alla riservatezza nel trattamento di dati personali in relazione e altri diritti fondamentali in Pubblica Amministrazione come il diritto alla trasparenza dell'azione amministrativa o il diritto all'accesso agli atti;

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

- estendere il programma formativo oltreché agli incaricati direttamente coinvolti nel trattamento dei dati, come previsto dal Disciplinare Tecnico, a tutte gli altri soggetti che a qualsiasi titolo interagiscono in questo processo.

I soggetti coinvolti nel Piano Formativo apparterranno alle seguenti categorie:

a) Amministratori dell'Ente (Sindaco, Assessori, Consiglieri)
b) Responsabili di Area/Servizio/Settore (e quindi Responsabili del Trattamento dei dati)
c) Incaricati del Trattamento
d) Amministratori di Sistema e Tecnici - Informatici che presiedono alla gestione del Sistema Informativo dell'Ente
e) Dipendenti Tutti, Lavoratori a Progetto, Professionisti convenzionati

La formazione verrà erogata sia al momento dell'ingresso in servizio, che in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Le tematiche trattate saranno le seguenti:

1) Sensibilizzazione sulle problematiche legate alla tutela della riservatezza e sulla loro importanza Analisi e studio della Politica di Sicurezza in materia che l'Ente intende attuare La formazione avrà anche l'obiettivo di trasmettere il messaggio che la tutela della privacy, che di per sé costituisce adempimento ad obbligo normativo, potrà anche contribuire a garantire l'Ente dal rischio di perdita o comunque compromissione del lavoro svolto dagli uffici;

2) Formazione sugli aspetti generali della Norma e sull'adeguamento alla stessa sia in presenza di archivi cartacei che di banche dati elettroniche;

3) Formazione sull'analisi dei rischi, con riferimento alle Misure di Sicurezza da adottare, sui contenuti del Disciplinare Tecnico in relazione ai trattamenti ed alle operazioni di manutenzione e ripristino dei dati ed ai diversi comportamenti da tenere ai diversi livelli di responsabilità sia nel quotidiano che nelle situazioni di emergenza;

4) Formazione sui contenuti tecnico informatici del Codice ed in particolare sulle prescrizioni contenute nel Disciplinare Tecnico (minacce, rischi, software, strumenti anti-intrusione, backup, supporti rimovibili, etc).

I Soggetti saranno coinvolti nelle tematiche sopra esposte come da prospetto che segue:

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Soggetti		Tematiche			
		1	2	3	4
a)	Amministratori	☐			
b)	Responsabili di Area	☐	☐		
c)	Incaricati		☐	☐	☐
d)	Amministratore di Sistema e Tecnici - Informatici			☐	☐
e)	Dipendenti Tutti	☐	☐	☐	☐

Matrice di Correlazione Soggetti - Tematiche

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Sezione 9 Trattamento di dati personali affidati all'esterno Regola 19.7 Allegato B al D. Lgs. 196/03

Disciplinare Tecnico

Il titolare provvede a descrivere i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

Qualora l'Ente proceda ad affidare all'esterno (a Società, Cooperative, Liberi Professionisti ecc) la gestione di Servizi o Attività che comportino il trattamento di dati personali, è necessario che il soggetto al quale viene affidato l'incarico rilasci specifiche garanzie (anche assumendo l'obbligo in sede di stipula della convenzione o del contratto con cui si disciplina l'affidamento del Servizio o della attività) al Comune con riferimento al rispetto del D. Lgs. 196/03 nelle operazioni di trattamento dei dati personali.

In particolare, il soggetto esterno al quale viene affidato il trattamento dei dati da parte del Comune deve impegnarsi a:

- Trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto;
- Adempiere a tutti gli obblighi previsti dal Codice per la protezione dei dati personali (D. Lgs. 196/03);
- Comunicare il nominativo del soggetto (persona fisica) Titolare del trattamento dei dati e, se presenti, il nominativo dei soggetti individuati quali Responsabili del trattamento dei dati;
- Rispettare le istruzioni specifiche eventualmente ricevute dal Comune per il trattamento dei dati personali;
- Relazionare periodicamente sulle misure di sicurezza adottate e informare immediatamente l'Ente in caso di situazioni anomale o di emergenza.

Con riferimento al trattamento di dati personali dell'Ente, affidati a soggetti esterni allo stesso, si procederà secondo le prescrizioni contenute nella presente Sezione e riassunte nella tabella che segue.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it
C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

Misura da adottare

Il soggetto esterno affidatario di operazioni di trattamento su Banche Dati dell'Ente fornirà le seguenti garanzie:

1 di essere consapevole che i dati che gestirà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, gli stessi potranno essere trattati ai soli fini dell'espletamento dell'incarico in essere con l'Amministrazione;

2 di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;

3. di adottare tutte le istruzioni specifiche eventualmente ricevute dall'Ente per il trattamento dei dati personali integrandole eventualmente con le procedure già in essere;

4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente l'Ente in caso di situazioni anomale o di emergenza;

5. di impegnarsi a stipulare idonea polizza assicurativa per Responsabilità Civile per un importo pari ad € 1.500.000,00 e di riconoscere il diritto dell'Ente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

SIPAL
Servizi Integrati alla Pubblica Amministrazione Locale
Scuola Regionale di Polizia Locale
Via S. Satta, 55 – 09128 Cagliari
Tel. 07042835 – 070401301 - Fax 0704529135
www.sipal.sardegna.it - info@sipal.sardegna.it

C.F. e P.I. 02848400921
C.S. € 90.000,00 (i.v.)
REA 228746

****

Letto, Confermato e Sottoscritto il 19 03 2008

Dott. Danilo Cannas