Comune di Ospedaletto Euganeo

Piazza Sandro Pertini, 8
35045 – Ospedaletto Euganeo (PD)

Tel: 0429-90684 Fax: 0429-90786
E-mail: ragioneria@comune.ospedalettoeuganeo.pd.it

Documento Programmatico sulla Sicurezza

Redatto in base alle disposizioni del
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
del
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(art.34 e Allegato B, regola 19, del d.lgs. 30 giugno 2003, 196)

PROVEDIMENTO DEL GARANTE DEL 27 NOVEMBRE 2008, G.U. n.300 del 24 dicembre 2008

Data ultima revisione documento: **04/12/2015**

Il titolare del trattamento
Il Sindaco
F-to Battistella Ing. Antonio

INDICE

1. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto in base alle disposizioni di cui al punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, ai sensi e per gli effetti dell' articolo 34, comma 1, lettera G) del DLGS 196 del 30 giugno 2003 (codice in materia di dati personali), e del disciplinare tecnico allegato al medesimo DLGS 196/2003 SUB B)

1.1 Periodicità di revisione del documento programmatico sulla sicurezza

Entro il 31 marzo di ogni anno, il **Titolare del trattamento** di dati sensibili o di dati giudiziari deve verificare ed aggiornare il **Documento programmatico sulla sicurezza** contenente idonee informazioni riguardo ai **punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).**

1.2 Scopo

Il presente Documento Programmatico Sulla Sicurezza è redatto per soddisfare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n. 196 del 30 giugno 2003).

Inoltre costituisce un valido strumento per la adozione delle misure previste **dall'Art. 31, dall'Art. 34 e dall'Art. 35** dello stesso **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.

Scopo del presente Documento programmatico sulla sicurezza è quello di ridurre al minimo 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, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

1.3 Campo di applicazione

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i **dati personali: .**

- **Sensibili**
- **Giudiziari**
- **Comuni**

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il Documento programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.4 Riferimenti Normativi

1. Codice in materia di dati personali (D.lgs. n. 196 del 30 giugno 2003)
2. Disciplinare tecnico in materia di misure minime di sicurezza (Artt. Da 33 a 36 del codice
3. Provvedimento del garante del 27 novembre 2008 pubblicato su g.u. n. 300 del 24 dicembre 2008

1.5 Elenco degli allegati e dei modelli utilizzati

Al fine di evitare duplicazioni e per consentire un più agevole aggiornamento periodico del presente documento, l' Ente ha stabilito di inserire come allegati alcuni documenti che potranno essere modificati anche in corso di validità del presente documento in modo da garantire la piena rispondenza del documento di sicurezza con la situazione in essere.

Gli allegati per motivi di sicurezza non saranno pubblicati ma saranno a disposizione per chi ne farà richiesta motivata.

Allegati:

Allegato 1	Schede Trattamenti
Allegato 2	Trattamenti per ufficio

1.6 Definizioni

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza I'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, I'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

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 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, nonché 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'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato odi indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

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.

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.

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.

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.

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.

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.

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.

Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

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.

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.

Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonche i trattamenti ad essa consentiti.

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.

2 . RUOLI, COMPITI E NOMINA DELLE FIGURE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI

2.1 Titolare del trattamento dei dati personali

Il Titolare del trattamento dei dati personali

Denominazione	Comune di Ospedaletto Euganeo
Indirizzo sede legale	Piazza Sandro Pertini, 8 35045 – Ospedaletto Euganeo (PD)
Rappresentante legale	Sindaco: ing. Antonio Battistella

Compiti del titolare del trattamento dei dati personali

In base a quanto stabilito dall'**Art. 4, comma 1, lettera f) del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** il "***Titolare del trattamento*** *è 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*".

Il **Titolare del trattamento** si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)** tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il **Titolare del trattamento** può decidere, qualora lo ritenga opportuno, di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)**, il **Titolare del trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del trattamento** anche mediante suddivisione di compiti.

I **Responsabili del trattamento** sono individuati 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.

I compiti affidati ai **Responsabili del trattamento** sono analiticamente specificati per iscritto dal **Titolare del trattamento**.

I **Responsabili del trattamento** effettuano il trattamento attenendosi alle istruzioni impartite dal **Titolare del trattamento**.

- In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** il **Titolare del trattamento**, in relazione

all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili della sicurezza dei dati** che assicurino e garantiscano che vengano adottate tutte le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**.

- Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dati**, ne assumerà tutte le responsabilità e funzioni.

- In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili di specifici trattamenti** con il compito di individuare, nominare e incaricare per iscritto, gli **Incaricati del trattamento dei dati personali**.

2.2. Amministratore di Sistema, Base dati e Rete

Compiti degli Amministratori di Sistema, Base dati e Rete

In base a quanto stabilito dal Provvedimento a carattere generale del 27 novembre 2008 pubblicato nella G.U. n. 300 del 24 dicembre 2008, il Titolare del trattamento, in presenza di di sistemi software complessi, deve designare uno o più soggetti **Amministratori di sistema**, Amministratori di base dati e Amministratori di rete anche mediante suddivisione di compiti, laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza, oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici

cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.
Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.
L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

L' Amministratore di sistema ha il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Individuare, nominare e incaricare per iscritto, uno o più Incaricati della gestione e della manutenzione degli strumenti elettronici.
- Ai sensi del Provvedimento del Garante del 27/11/2008 comma 2 lettera f, adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

L' Amministratore di base dati ha il compito di:

- Individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati.
- Individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali.
- Custodire e conservare i supporti utilizzati per le copie dei dati.
- Ai sensi del Provvedimento del Garante del 27/11/2008 comma 2 lettera f, adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

L' Amministratore di rete ha il compito di:

- Gestire e mantenere le connessioni di rete aziendali, garantendone la funzionalità e la sicurezza specie nei contesti nei quali queste siano interfacciate con altre reti pubbliche o private

Qualora il Titolare del trattamento ritenga di non nominare alcun Amministratore di sistema, Amministratore di base dati, Amministratore di rete, ne assumerà tutte le responsabilità e funzioni.

Il Titolare del trattamento informa che

Egli ha la facoltà di prevenire ed accertare eventuali accessi non consentiti ai dati personali e con cadenza per lo meno annuale verificare la rispondenza dell'operato dell'Amministratore di Rete in merito alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali

Viene precisato inoltre che se l'incarico di Amministratore di sistema, Amministratore di base dati, Amministratore di rete è affidato in outsourcing, il Titolare del trattamento ai sensi del Provvedimento del Garante del 27/11/2008 comma 2 lettera d ha l'obbligo di conservare direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di base dati

Nomina dell'Amministratore di sistema, Amministratore di base dati, Amministratore di rete

La nomina di uno o più Amministratore di sistema, Amministratore di base dati, Amministratore di rete, deve essere effettuata dal Titolare del trattamento con un incarico ufficiale in cui sono specificate le responsabilità che gli sono affidate.

Copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

Il Titolare del trattamento deve informare ciascun Amministratore di sistema, Amministratore di base dati, Amministratore di rete,delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n.196 del 30 giugno 2003) e del Provvedimento del Garante del 27 novembre 2008.

Il Titolare del trattamento deve consegnare a ciascun Amministratore di sistema, Amministratore di base dati, Amministratore di rete, una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina degli Amministratori sopra menzionati è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina degli Amministratori sopra menzionato può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

L'amministratore di sistema

Il Comune ha individuato una unica persona che evidenzia tutte le figure di Amministratore di sistema per l'Ente. Gli accessi alle aziende esterne di manutenzione verrà assegnata secondo i

dettagli contrattuali con le aziende fornitrici e subordinati alla approvazione e alla supervisione dell'amminstratore di sistema.

Denominazione	Rapporto	Rapporto
Giancarlo Moro	Dipendente comunale	Amministratore di sistema Amministratore di rete Amministratore di basi dati

2.3 Responsabile del trattamento dei dati personali

Compiti del responsabile del trattamento dei dati personali

Il Responsabile del trattamento dei dati personali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti.

- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco dei trattamenti dei dati personali.
- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
- Nominare un responsabile o almeno un incaricato con il compito di controllare i sistemi, le apparecchiature e l'accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
- Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati e custodire e conservare i supporti utilizzati per le copie dei dati

Il **Titolare**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili del trattamento dei dati con il compito di individuare, nominare e incaricare per iscritto, gli Incaricati del trattamento dei dati personali.

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)**, il **Titolare del trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del trattamento dei dati** anche mediante suddivisione di compiti.

I Responsabili del trattamento dei dati sono individuati 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.

Il Responsabile del trattamento dei dati personali ha il compito di:

- Nominare gli incaricati del trattamento per i trattamenti di dati che gli sono state affidati.
- Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003**.

- Dare le istruzioni adeguate agli **Incaricati del trattamento** effettuato con strumenti elettronici
- Dare le istruzioni adeguate agli **Incaricati del trattamento** effettuato senza l'ausilio di strumenti elettronici
- Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli **Incaricati del trattamento dei dati personali.**

Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile del trattamento dei dati personali, ne assumerà tutte le responsabilità e funzioni.

Nomina del responsabile del trattamento dei dati personali

La nomina di ciascun Responsabile del trattamento dei dati personali deve essere effettuata dal Titolare del trattamento con un atto ufficiale di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per ricevuta.

Copia della nomina deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

Il Titolare del trattamento deve informare ciascun Responsabile del trattamento dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina del Responsabile del trattamento dei dati personali è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile della trattamento dei dati personali può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

I Responsabile del trattamento dei dati personali del Comune di Ospedaletto Euganeo

Il Titolare ritenuto opportuno, in relazione a quanto previsto dall'art. 29 comma 4 del d.lgs. 196/2003, specificare analiticamente i compiti e le responsabilità affidati a ciascun Responsabile nomina come responsabili del trattamento dei dati i singoli responsabili individuando per ciascuno i trattamenti cui sottoporre la loro responsabilità.

Ogni nomina individua i settori ed i trattamenti di responsabilità del singolo responsabile. Tutti i Responsabili dovranno collaborare tra di loro in armonia e collaborazione con il Responsabile della gestione e della manutenzione degli strumenti elettronici.

L' allegato 1 contiene l'elenco dei responsabili al trattamento dei dati con il dettaglio dei trattamenti affidati.

2.4 Incaricato della custodia delle copie delle credenziali

Compiti degli incaricati della custodia delle copie delle credenziali

In conformità a quanto disposto dal **punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** debbono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il **Titolare del trattamento** 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.

E' onere del **Titolare del trattamento** o, se designato, del **Responsabile del trattamento dei dati personali**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della custodia delle copie delle credenziali**.

E' compito degli **Incaricati della custodia delle copie delle credenziali:**

- Prendere atto della assegnazione delle Credenziali di autenticazione per l'accesso ai dati personali degli Incaricati del trattamento, su richiesta del Responsabile dello specifico trattamento, avvalendosi del supporto tecnico del Responsabile della gestione e della manutenzione degli strumenti elettronici, in conformità a quanto disposto dal punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.**
- Assicurare che il Codice per l'identificazione, laddove sia stato già utilizzato, non sia assegnato ad altri Incaricati del trattamento, neppure in tempi diversi, in conformità a quanto disposto dal punto 6 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)
- Verificare la revoca delle Credenziali di autenticazione per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 3 (tre) mesi, in conformità a quanto disposto dal punto 7 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003).
- Verificare la revoca di tutte le Credenziali di autenticazione non utilizzate in caso di perdita della qualità che consentiva all'Incaricato del trattamento l'accesso ai dati personali, in conformità a quanto disposto dal punto 8 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003).

In caso di prolungata assenza o impedimento di un **Incaricato del trattamento** che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'**Incaricato della custodia delle copie delle credenziali,** in accordo con il **Responsabile del trattamento di dati personali** può assicurare la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. In caso di possibile modifica delle credenziali da parte dell' amministratore dei sistemi informativi senza conoscenza delle credenziali:
    a. Chiedere all' amministratore di sistema di utilizzare i diritti di "amministratore di sistema", per modificare in modo forzoso la **componente riservata delle credenziali di autenticazione** dell'**Incaricato del trattamento dei dati personali** assente o impedito ad effettuare il trattamento.
    b. Comunica la **componente riservata delle credenziali** di autenticazione così modificata ad un altro **Incaricato del trattamento dei dati personali** designato dal **Responsabile dello specifico trattamento di dati personali** il quale potrà utilizzarla solo temporaneamente

c. Terminata l'assenza o l'impedimento dell'**Incaricato del trattamento** che aveva reso indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quest'ultimo dovrà essere informato dell'intervento effettuato e dovrà modificare la propria

Qualora il **Responsabile del trattamento dei dati personali** ritenga di **non** nominare alcun **Incaricato della custodia delle copie delle credenziali,** ne assumerà tutte le responsabilità e funzioni.

Nomina degli incaricati della custodia delle copie delle credenziali

In conformità a quanto disposto dai punti 3, 4, 5, 6, 7, 8, 9 e 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003), il Responsabile del trattamento dei dati personali nomina uno o più soggetti Incaricati della custodia delle copie delle credenziali a cui è conferito il compito di autorizzare l'assegnazione e la gestione delle Credenziali di autenticazione per l'accesso ai dati gestiti con strumenti elettronici.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** deve essere effettuata con una lettera di incarico, deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile del trattamento dei dati personali** in luogo sicuro.

Il **Responsabile del trattamento dei dati personali** deve informare gli **Incaricati della custodia delle copie delle credenziali** della responsabilità che è stata loro affidata in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n.196 del 30 giugno 2003)**.

Il Responsabile del trattamento dei dati personali deve consegnare a ciascun Incaricato della custodia delle copie delle credenziali, una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** può essere revocata in qualsiasi momento dal **Responsabile del trattamento dei dati personali** senza preavviso, ed essere affidata ad altro soggetto.

Gli incaricati della custodia delle copie delle credenziali

Il titolare decide di nominare come incaricati delle copie delle credenziali

Denominazione	Rapporto
Giancarlo Moro	Dipendente comunale

2.5 Incaricato del trattamento dei dati personali

Compiti degli incaricati del trattamento dei dati personali

In base a quanto stabilito dall'**Art. 30 del Dlgs. n.196 del 30 giugno 2003**, le operazioni di trattamento possono essere effettuate solo da **Incaricati del trattamento** che operano sotto la diretta autorità del **Titolare del trattamento** o, se designato, del **Responsabile di uno specifico trattamento di dati personali**, attenendosi alle istruzioni impartite.

In base a quanto definito dall'**Art. 4, punto 1, comma h) del Dlgs. n.196 del 30 giugno 2003**, gli *"**Incaricati del trattamento** sono persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Titolare del trattamento** o, se designato, dal **Responsabile di uno specifico trattamento di dati personali**"*.

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.
- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.
- L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- Gli Incaricati del trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'Incaricato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni tre mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.
- Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

Nomina degli incaricati del trattamento dei dati personali

Preso atto che l'art. 30 del d.lgs. 196/2003 dispone che:

1. 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.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una

unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima;

La nomina di ciascun **Incaricato del trattamento dei dati personali** deve essere effettuata dal **Responsabile del trattamento dei dati** con un **provvedimento di incarico** in cui sono specificati i compiti che gli sono stati affidati.

Il **Responsabile del trattamento dei dati** deve informare ciascun **Incaricato del trattamento dei dati personali** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Gli **Incaricati del trattamento dei dati personali** devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli **Incaricati del trattamento dei dati personali** deve essere assegnata **una parola chiave** e **un** codice di autenticazione informatica.

Agli **Incaricati del trattamento dei dati personali** è prescritto di adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina di ciascun Incaricato del trattamento dei dati personali deve essere effettuata dal Titolare del trattamento o da un Responsabile del trattamento dei dati con un atto ufficiale di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per ricevuta.

La nomina **dell'Incaricato del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'Incaricato del trattamento dei dati personali può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

Gli Incaricati del trattamento dei dati personali del Comune di Ospedaletto Euganeo

Il Titolare ritenuto opportuno, in relazione a quanto previsto dall'art. 29 comma 4 del d.lgs. 196/2003, specificare analiticamente i compiti e le responsabilità affidati a ciascun Responsabile nomina come responsabili del trattamento dei dati i singoli responsabili individuando per ciascuno i trattamenti cui sottoporre la loro responsabilità.

Ogni nomina individua i settori ed i trattamenti di responsabilità del singolo responsabile. Tutti i Responsabili dovranno collaborare tra di loro in armonia e collaborazione con il Responsabile della gestione e della manutenzione degli strumenti elettronici.

Codice	Cognome	Nome
1	Nola	Lucia
2	Binato	Simonetta
3	Delaiti	Elisa
4	Ferrarato	Francesco

Codice	Cognome	Nome
5	Facciolo	Federica
6	Andreetto	Antonella
7	Zanin	Alberto
8	Merlo	Patrizia
9	Franchin	Anna Sofia
10	Zennaro	Lucia

L’ allegato 2 contiene la suddivisione dei trattamenti per responsabilità e incarico.

3. ANALISI DELLA SITUAZIONE E DEI RISCHI

Il Comune di Ospedaletto Euganeo è organizzato in settori e servizi a cui fanno capo alcuni responsabili. Il lavoro è suddiviso in una unica sede e le postazioni sono collegate tra loro tramite una rete estesa che utilizza un protocollo ethernet.

3.1 Elenco dei trattamenti

L'elenco dei trattamenti è stato rilevato con la collaborazione di tutti i responsabili del comune. E' stata compilata una scheda dettagliata relativa ai dati personali trattati. Per tutti i trattamenti si è evidenziata la normativa autorizzatoria all'utilizzo dei dati.

In allegato (allegato 1) è evidenziato l'elenco ed il dettaglio dei trattamenti. Ogni trattamento ha un responsabile del trattamento ben individuato e i propri incaricati.

3.2 La mappa dei trattamenti effettuati

In allegato 2 vengono elencati i trattamenti effettuati dai diversi uffici. In questo paragrafo si considerano le sintesi dei trattamenti effettuati

In relazione al diverso grado di rischio, è opportuno distinguere i trattamenti che vengono posti in essere nelle distinte aree in cui sono dislocati gli strumenti, nei casi in cui la circostanza è significativa (per gli schedari e gli elaboratori non in rete).

Nelle caselle di incrocio si appone un simbolo **X**, che sta a significare che determinati tipi di dati sono trattati con determinati strumenti.

TIPI DI DATI TRATTATI				
Dati comuni relativi a utenti (cittadini, contribuenti)	X	X	X	
Dati comuni relativi a fornitori e clienti	X		X	
Dati sensibili relativi a utenti	X		X	
Dati comuni relativi ad altri soggetti	X		X	
Dati relativi allo svolgimento di attività economiche e di pubblica utilità	X		X	X
Dati relativi al personale, nonché a candidati per diventarlo, anche sensibili	X		X	
	A	**B**	**C**	**D**
	STRUMENTI UTILIZZATI			

Legenda degli strumenti utilizzati per il trattamento:
A – Schedari ed altri supporti cartacei
B – Elaboratori non in rete
C – Elaboratori in rete privata
D – Elaboratori in rete pubblica

I dati sensibili sono gestiti in maniera elettronica su Personal Computer in rete e in maniera cartacea come i dati personali non sensibili.

Il sito web contiene dati personali solo relativi ad attività istituzionali o di dati di cui è stata chiesta l'autorizzazione.

L' accesso al portale web è protetto.

Da una analisi più dettagliata di tutti i trattamenti si può notare come la gestione dei dati sensibili in formato elettronico avvenga con l' utilizzo di procedure informatizzate ospitate su server centrali protetti, mentre la grande quantità di banche dati locali (sui singoli PC) fanno riferimenti a dati non sensibili

Da una analisi della gestione degli archivi cartacei si può notare come talvolta la protezione dei documenti, anche quelli contenenti dati sensibili, sia affidata ad armadi non dotati di chiusure

3.3 Locali

Le sedi degli uffici comunali considerati nel presente Documento Programmatico sulla sicurezza sono:

Codice	Sede	Indirizzo
001	Sede Municipale	Piazza Sandro Pertini, 8

Essendo per sua natura un Ente di pubblica utilità esistono delle vaste aree in cui l'accesso ai locali è consentito liberamente al pubblico che deve utilizzare i pubblici servizi senza passare particolari controlli per accedere alle aree.

L'accesso agli uffici è comunque controllato dagli operatori che sono istruiti a non consentire l'accesso agli estranei nelle zone di lavoro.

3.4 Sistema informatico

Il sistema informatico del Comune di Ospedaletto Euganeo è costituito da tre componenti:

- l'infrastruttura di rete
- i server
- i client

L' infrastruttura di rete

La sede è tutte cablata con rete ethernet i cui apparati attivi sono disposti in un armadio non accessibile.

Il cuore della rete è posizionato attualmente presso la sala server posta al terzo piano e in una stanza chiusa a chiave.

La sede è collegata ad internet protetta da firewall.

Tutto il sistema è protetto da un sistema antivirus centralizzato

L'accesso alla rete tramite Active directory

Struttura del Direttorio

La struttura adottata per il direttorio AD si basa sulla creazione di un unico dominio con due macchine che permettono di avere il backup della struttura di rete (windows 2003). Il dominio dal punto di vista dell'architettura AD è un unico "sito", un'unica "foresta" e un unico "spazio dei nomi".

Servizi integrati

Allo stato attuale l'accesso alla struttura di dominio da parte degli utenti del Comune rende disponibili i seguenti servizi di base:

1. Verifica delle credenziali di accesso al Personal Computer;
2. Accesso alla rete Internet (solo per gli utenti esplicitamente abilitati) con le stesse credenziali;
3. Accesso ad un'area di memorizzazione personale (home) su file server;

4. Accesso ad un'area di memorizzazione comune (per ufficio) su file server;
5. Accesso ad aree di memorizzazione di supporto ad applicativi installati (aggiornamenti, file comuni, ecc) secondo le applicazioni configurate sulla stazione utente;
6. Accesso ad altre aree comuni su FileServer secondo esigenze rilevate di volta in volta.

Per tutti le aree rese disponibili su FileServer è previsto un salvataggio giornaliero delle informazioni.

I server

I server di rete sono di tre tipologie:

1. Sistema IBM i-series AS/400 attualmente posizionato presso la sala CED
2. Sistemi server con piattaforma Intel dotati di sistema operativo Windows 2003 posizionati presso presso la sala CED
3. Apparati firewall e router presso la sala CED

I server sono posti tutti in locali non accessibili a personale non autorizzato e chiusi a chiave. L'accesso ai locali è permesso solo se accompagnati da personale appositamente autorizzato.
I locali sono dotati di sistema di climatizzazione e protetti da sistemi di controllo di potenza elettrica (UPS) che garantiscono continuità alla alimentazione dei server. Questo garantisce da arresti improvvisi dei servizi e diminuisce il rischio di rotture accidentali dei sistemi.

Per i server windows è gestito un unico dominio di sistema.

Tutti gli utenti di rete sono autenticati sia al dominio che ai vari server gestionali per l'impossibilità di implementare in tempi brevi il single sign-on.

L'accesso al server **AS/400** avviene in due modalità:

1. Accesso del PC alla connessione con il sistema, per questo avviene il collegamento con utente generico che ha come unica autorizzazione il collegamento al sistema. Tale utente generico non può effettuare altre operazioni
2. Accesso al sistema: ogni utente è fornito di proprie credenziali con cui accedere ai vari applicativi o banche date di sistema

Il server di posta prevede la gestione di credenziali autonome e ben definite.

Tutti i server sono protetti da un sistema centralizzato di antivirus che provvede automaticamente all' aggiornamento

L'elenco dei sistemi è allegato al presente documento ed è costantemente aggiornato dal responsabile della sicurezza dei sistemi elettronici

I client (personal computer e terminali)

L'elenco dei personal computer è mantenuto in un database a cui può accedere solo il responsabile alla sicurezza dei dati e l'incaricato alla manutenzione dei sistemi.

Esso contiene tutte le informazioni relative a :

- nome computer
- tipo computer
- sistema operativo
- software installato

Non si riporta in allegato tale elenco in quanto in continua evoluzione.

Tutti i computer (client) collegati alla rete hanno sistema operativo windows XP o windows 2000 nelle versioni professional che garantiscono la possibilità di collegamento al dominio e rendono minime le possibilità di collegarsi anche ai singoli dati del computer se privi di password di accesso.

Tutti i computer sono dotati di manutenzione hardware e permettono l'accesso solo se autenticati dal dominio

Il software di gestione

I software per la gestione dei dati sono in regolare manutenzione con le case produttrici e l'attività di gestione delle banche dati avviene solo tramite autorizzazione dell'Amministratore di Sistema

I responsabili del trattamento dei dati istruiranno in maniera opportuna gli incaricati ed eventualmente il responsabile della manutenzione dei sistemi elettronici di assegnare ai singoli utenti un profilo di utilizzo personalizzato secondo le autorizzazioni prospettate.

3.5 Schedari ed altri supporti cartacei

I supporti cartacei, ivi inclusi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo.

Ogni ufficio ha il dettaglio del contenuto dei singoli armadi. Tale elenco è al momento non riproducibile nel dettaglio nel presente documento

Per gli archivi chiusi a chiave contenente dati sensibili le chiavi sono date a ciascun incaricato della gestione dei dati e non sono a disposizione del pubblico.
Ogni volta che un operatore si allontana dalla stanza in cui sono presenti gli armadi provvede a chiudere l'armadio sotto il suo controllo.

3.6 Mansionario privacy ed interventi formativi degli incaricati

Per il trattamento dei dati personali, il Titolare:

ha nominato i responsabili per il trattamento dei dati, attribuendo loro incarichi di ordine organizzativo e direttivo, come*:*

- responsabile per la sicurezza, il cui compito è di progettare, realizzare e mantenere in efficienza le misure di sicurezza, conformemente a quanto previsto dagli articoli 31 e 33 Dlgs 196/2003, nelle persone dei dirigenti del Comune di Ospedaletto Euganeo.

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne, in caso sia necessario, una copia al preposto alla custodia delle parole chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa, nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nell'allegato 2 vengono riportati in dettaglio i livelli di accesso a cui sono autorizzati i vari appartenenti ad uffici o unità operative.

Sono stati effettuati degli **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono stati effettuati mediante corso in aula e messa a disposizione del materiale informativo

I corsi di formazione

Sono stati effettuati i corsi di formazione a quasi tutto il personale dipendente e affiliato.
Alle poche persone non presenzianti al corso è stata fatta formazioni dai colleghi sfruttando il materiale a corredo del corso messo a disposizione nella intranet comunale

Periodicamente vengono organizzati all' interno della struttura corsi di informazione e formazione relativa al corretto utilizzo dei prodotti informatici

3.7 Analisi dei rischi che incombono sui dati

Il **Responsabile del trattamento dei dati personali** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, anche avvalendosi di consulenti interni o esterni, deve verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Nell'analisi dei rischi si devono considerare gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali.

Tipologia di rischio

Si evidenziano tre categorie di rischi e per ognuna si considerano le azioni che possono essere più dannose per i dati

1) comportamenti degli operatori:

	Azione	Descrizione	Impatto
E001	sottrazione di credenziali di autenticazione	Le credenziali (userID Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso	Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto.
E002	errore materiale, carenza di consapevolezza, disattenzione o incuria	A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.
E003	comportamenti sleali o fraudolenti	Con comportamento consapevole, derivate potenzialmente da vari fattori quali (risentimenti verso l'Ente, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati

2) eventi relativi agli strumenti:

	Azione	Descrizione	Impatto
E004	azione di virus informatici o di programmi suscettibili di recare danno	Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può essere venirsi ad installare o essere semplicemente eseguito del software spurio del tipo "virus" informatico.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
E005	spamming o tecniche di sabotaggio	Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta spuria generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie.	Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari.
E006	malfunzionamento, indisponibilità o degrado degli strumenti	I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati.

		cui possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.	
E007	accessi esterni non autorizzati	Soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW/SW da cui e possibile intervenite su una banca dato obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati
E008	intercettazione di informazioni in rete	Soggetti malintenzionati possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica dell'Ente. Ciò può avvenire in un qualunque tra il sistema utilizzato e il sistema HW/SW degli incaricati.	Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.

3) eventi relativi al contesto fisico-ambientale:

	Azione	Descrizione	Impatto
E009	ingressi non autorizzati a locali/aree ad accesso ristretto	Un soggetto autorizzato allo scopo, può comunque accedere fisicamente ai locali presso dai quali è accessibile e manipolabile la banca dati interessata all'evento.	Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
E010	sottrazione di strumenti contenenti dati	I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente da parte di altri soggetti non aventi diritto di accedere a tale banca dati.	L'evento comporta la sottrazione, in modo illecito, di dati.
E011	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria	I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa.	Dall'evento può derivare la distruzione totale o parziale della banca dati.

E012	guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)	I sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata o che contiene la banca dati interessata all'evento possono avere malfunzionamenti i conseguenza di varie cause.	Dall'evento può derivare la distruzione totale o parziale della banca dati.
E013	errori umani nella gestione della sicurezza fisica	Nella messa in opera della gestione della sicurezza può accadere chele persone dedicate al loro rispetto facciano degli errori nella loro messa in atto o non le portino a compimento	In caso di forzatura della messa in sicurezza non effettuata possono avvenire sottrazione o perdite di dati

Probabilità e impatto sulla sicurezza

Con la seguente matrice si procede a una stima del grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

GRADO DI INTERESSE PER I TERZI	**ELVATISSIMO**				Dati di natura genetica
	ALTO				Dati affezione da virus HIV
	MEDIO	Dati comuni, cittadini, utenti consumatori, elettori	Dati svolgimento di attività economiche	Dati sensibili clienti utenti membri pazienti	Dati stato di salute e/o vita sessuale
	BASSO	Dati comuni di fornitori	Dati biometrici clienti personale Dati idonei a rilevare la posizione	Dati di natura giudiziari a Dati sensibili personale	
		BASSO	**MEDIO**	**ALTO**	**ELEVATISSIMO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati

	Evento	Probabilità (1=bassa-4=elevata)	Impatto sulla sicurezza (gravità: 1=bassa-4=elevata)	Rischio (PXG)
E001	sottrazione di credenziali di autenticazione	1	2	2
E002	errore materiale, carenza di consapevolezza, disattenzione o incuria	1	1	1
E003	comportamenti sleali o fraudolenti	1	2	2

E004	azione di virus informatici o di programmi suscettibili di recare danno	1	3	3
E005	spamming o tecniche di sabotaggio	1	2	2
E006	malfunzionamento, indisponibilità o degrado degli strumenti	1	1	1
E007	accessi esterni non autorizzati	1	3	3
E008	intercettazione di informazioni in rete	1	2	2
E009	ingressi non autorizzati a locali/aree ad accesso ristretto	2	2	4
E010	sottrazione di strumenti contenenti dati	2	2	4
E011	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria	1	2	2
E012	guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)	1	2	2
E013	errori umani nella gestione della sicurezza fisica	2	2	4

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere idealmente suddivise in:

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti)
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)
3. rischio di penetrazione logica nelle reti di comunicazione
4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali. Il simbolo **o**, posto nella casella di intersezione, significa che l'esposizione al rischio è modesta; il simbolo **O** significa che l'esposizione al rischio è elevata

TIPI DI DATI TRATTATI

Rischio d'area, legato al verificarsi di eventi distruttivi	O		o	
Rischio d'area, legato all'accesso non autorizzato nei locali	O		o	o
Rischio di guasti tecnici di hardware, software e supporti		o	o	o
Rischio di penetrazione logica nelle reti di comunicazione				o
Rischio legato ad atti di sabotaggio e ad errori umani	o	o	O	o

A	B	C	D
STRUMENTI UTILIZZATI			

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei
B – Elaboratori non in rete
C – Elaboratori in rete privata
D – Elaboratori in rete pubblica

Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:

- il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato inferiore per l'area ad accesso controllato (uffici di back-office), rispetto a quanto accade per le aree di contatto con il pubblico
- il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti non in rete (pc portatili) che, essendo affidati a singoli che non sempre possiedono un bagaglio tecnico adeguato, presentano un rischio di rottura maggiore, rispetto agli impianti che vengono gestiti da persone con specifiche competenze,oltre alla possibilità di essere trafugati
- il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico, gli unici elaboratori collegati alla rete sono in una rete demilitarizzata e e contengono solo il server di posta con apposito software antivirus a cui si accede solo tramite le porte abilitate dal router e dal server web con apposita protezione degli accessi
- il rischio legato ad atti di sabotaggio, o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati, è maggiore per quelli che sono in rete.

4. MISURE DI SICUREZZA

Nel presente capitolo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal Dlgs 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

4.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da:

- dispositivi antincendio come da obblighi relativi ai sensi del Dlgs 626/94 e successive modifiche
- i sistemi server sono protetti da gruppi di continuità dell'alimentazione elettrica
- la maggior parte dei locali è dotata di impianto di condizionamento che garantisce il rispetto delle condizioni adatte al mantenimento elettrico delle apparecchiature

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati non è possibile dotare l' Ente di particolari misure di prevenzione.

Gli strumenti a disposizione sono:

- sistema di allarme programmato negli uffici anagrafe, economato, e sala CED, collegato ad un istituto privato di Vigilanza per il pronto intervento
- chiusura dei locali al di fuori dell' orario di lavoro con porte non blindate
- servizio di vigilanza garantita dalla pubblica sicurezza
- finestre al piano terra di tipo antisfondamento e sul retro dotate di inferriate metalliche

Gli impianti ed i sistemi di cui è dotata l'organizzazione:
appaiono sufficienti, al fine di garantire le misure minime di sicurezza.

Appare necessario indicare le seguenti indicazioni per ogni locale in cui avviene un trattamento di dati:

- si devono responsabilizzare gli incaricati a proteggere il patrimonio dati in loro custodia seguendo le indicazioni per la gestione dei documenti cartacei, per la gestione degli strumenti elettronici.
- si devono responsabilizzare gli incaricati ad un uso consapevole dei locali a loro affidati tenendo chiuse le porte in loro assenza, chiudendo a chiave correttamente gli archivi ed evitando di far accedere agli uffici personale non autorizzato

Per la gestione degli archivi non essendoci impianti di allarme nei locali deve essere prevista al più presto una dotazione di chiusure per gli armadi che ne fossero privi.
Per gli armadi in vetro contenenti archivi si dovrà fare in modo che i faldoni contenenti documenti siano con dorso "anonimo" o almeno non riferito a dati personali.

4.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione.

A tale fine, gli incaricati sono stati dotati di

- cassetti con serratura
- armadi chiudibili a chiave
- armadi chiudibili

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi , armadi , casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti:

- ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede
- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'incaricato che ha il compito di custodirla
- la localizzazione dei documenti nei vari armadi è ben definita e conosciuta alle sole persone autorizzate. Non è possibile un accesso ai documenti non autorizzati "per errore" o per mancanza di conoscenza della disposizione degli archivi

- in caso di armadi chiusi a chiave è individuato per ogni archivio uno o più incaricati custode delle chiavi che sarà abilitato a chiudere ed aprire l'armadio quando serve
- gli armadi possono rimanere chiusi senza serratura solo in presenza di personale incaricato che controllerà eventuali accessi

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari appaiono appena sufficienti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti.

Si deve sottolineare la mancanza di chiusure di molti armadi contenenti dati sensibili. Per queste situazioni si deve prevedere a breve la modifica degli armadi in dotazione verificando la possibilità di inserire meccanismi di chiusura aggiuntivi oppure il trasferimento in altri locali non raggiungibili da personale non autorizzato.

Sarà dovere dei singoli incaricati comunicare ai responsabili del trattamento dei dati personali eventuale difformità o malfunzionamento dei sistemi di chiusura degli archivi.

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.

Il sistema di **autenticazione informatica** è delineato nella sezione "L'accesso alla rete tramite Active directory" .

Tutti i computer periferici sono dotati di sistema operativo windows XP e windows 2000 collegati al dominio ed hanno la possibilità di definire una identificazione che protegge anche i dati locali, consentendo di abilitare alle risorse interne gruppi ben definiti di persone.

Le password di rete vengono fornite dal servizio sistemi informativi e vengono modificate dagli utenti secondo le politiche citate. Per gli applicativi è possibile definire per ciascuno le proprie password. Ogni procedura prevede di definire dei ruoli di accesso che consentono di utilizzare solo i dati a cui si è autorizzati.

Per realizzare le credenziali di autenticazione si utilizzano i seguenti metodi:

si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla (se possibile), mantenerla riservata e modificarla periodicamente

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

ad ogni incaricato esse vengono assegnate o associate individualmente, per cui **non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale**.

E' invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro tre mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  1. immediatamente, non appena viene consegnata loro da chi amministra il sistema
  2. successivamente, almeno ogni tre mesi.
- Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.
- Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:
  1. esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, pippobaudo….)
  2. buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica e che vengano utilizzati sia caratteri maiuscoli che minuscoli.
- La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati.
- In caso di necessità di accedere alle risorse di un utente è necessario procedere con questi passi:
  1. Verificare la necessità di accedere solo con il profilo della persona di cui non si hanno le credenziali
  2. Verificare la effettiva urgenza dell'accesso ai dati
  3. Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando le credenziali di una persona non presente il

responsabile dei trattamenti dei dati richiederà formalmente al responsabile dei sistemi informativi di creare una nuova password temporanea per l'accesso immediato.
4. Tale password sarà utilizzata solo allo scopo urgente e specifico
5. L'amministratore di sistema creerà una nuova password che comunicherà tempestivamente al solo titolare delle credenziali con l'opzione di obbligo immediato della password.
6. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.
7. Al ritorno del titolare delle credenziali dovrà essere avvisato e verificare che la password creata dall'amministratore sia effettivamente funzionante e dovrà modificarla tempestivamente. In caso di assenza prolungata del titolare delle credenziali l'amministratore di sistema potrà disabilitare temporaneamente le credenziali.

Sistema di autenticazione

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che:

Il profilo di autorizzazione viene in genere studiato per ogni singolo incaricato.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Sistema antiintrusione

Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il **primo aspetto** riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, si è dotati di idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento automatico.

I sistemi sono stati **dotati di idoneo software antivirus centralizzato** che ha la caratteristica di aggiornare le definizioni dei virus ogni giorno e di diffonderle ai sistemi periferici e di essere sempre attivo.

L'incaricato alla manutenzione dei sistemi dovrà controllare almeno una volta alla settimana di essere adeguatamente in linea con gli aggiornamenti scaricati in automatico dal sistema.

Il **secondo aspetto** riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, che il nuovo codice privacy ha reso obbligatoria per i casi in cui si trattino dati sensibili o giudiziari.

A tale riguardo si nota che:

è installato un **firewall** in manutenzione con azienda esterna che ha definite le regole di sicurezza di accesso ed uscita verso la rete.

I router di sistema sono abilitati a far uscire il traffico di rete.

Non sono possibili indirizzamenti diretti dall' esterno verso la rete interna

Il **terzo aspetto** riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi.

Al momento non si è ritenuto di impostare una attività di questo tipo in quanto troppo onerosa anche in rapporto alla scarsa probabilità di eventi di questo tipo

Supporti rimovibili

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

4.4 Le misure di sicurezza adottate

Elenco delle misure adottate

A. Realizzazione della struttura di "Dominio Active Directory" (gestione credenziali e componenti della rete);
   - Adeguamento del sistema di accesso alle stazioni PC;
   - Rinnovo del parco hardware
B. Potenziamento sistema di sicurezza perimetrale (Firewall);

C. Potenziamento infrastruttura di rete LAN e MAN;

A. Realizzazione della struttura di "Dominio AD"

L'attuale normativa vigente pone stringenti vincoli relativamente agli accessi ai sistemi informatici contenenti dati personali e sensibili imponendo una gestione delle credenziali secondo requisiti tecnici precisi (scadenza e obbligo della sostituzione, dimensione minima, ecc. Vedi "DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA").
Al fine di adempiere ai vincoli per gli accessi ai sistemi informatici e porre la base per un repertorio centralizzato delle credenziali (utilizzabile per l'integrazione di ulteriori applicazioni) è stato adottato il modello di gestione proposto dall'ambiente Microsoft denominato "Dominio Active Directory" o "Dominio".

Tale infrastruttura permette:

- La creazione di un repertorio centralizzato delle credenziali all'interno di una rete;
- La creazione di un repertorio centralizzato delle risorse della rete (PC, Stampanti);
- La definizione di tutte le politiche relative alle password richieste dalla normativa vigente;
- L'applicazione di politiche di utilizzo delle stazioni PC in termini di attività consentite o meno agli utenti (installazione di software, utilizzo di applicazioni, ecc.

Si è provveduto inoltre all'adeguamento, mediante sostituzione, di una quota consistente di postazioni di lavoro ormai obsolete e inadeguate in termini sia hardware che software all'implementazione dell'infrastruttura di "Domino".

Per limitare al minimo le problematiche in fase di adeguamento del meccanismo delle password è stato definita una scadenza programmata (per gruppi omogenei di utenti) delle password attualmente in uso per l'accesso alle postazioni PC.

Contestualmente gli utenti dovranno procedere alla sostituzione della propria password secondo i seguenti vincoli, che saranno rigorosamente verificati dal sistema automatico:

A) Deve essere di ALMENO 8 caratteri
B) Deve Contenere ALMENO una lettera Maiuscola
C) Deve Contenere ALMENO una lettera Minuscola
D) Deve contenere ALMENO un Numero
E) Non deve contenere il nome o il cognome dell'utente o sue parti

Es.

Utente mario.rossi

1) Mari1069 (ERRATA contiene una parte del nome Mario)
2) pippo345 (ERRATA contiene caratteri minuscoli e numeri ma non Maiuscoli)
3) Pipp345 (ERRATA solo 7 caratteri)
4) Pippo345 (CORRETTA contiene 8 caratteri, nessuna parte del nome e cognome, caratteri maiuscoli minuscoli e numeri)

N.B. Salvo richieste specifiche la credenziale ha una durata massima di 3 mesi passati i quali il sistema richiede la sua sostituzione.

Terminata la fase di sostituzione della password l'utente dovrà compilare correttamente il modulo di gestione password integrando con le credenziali per tutti gli applicativi in uso (gestione contabilità, personale , ecc.). Il numero di credenziali gestite dall'utente potrà

comunque progressivamente diminuire in fase di integrazione delle singole applicazioni con il "Dominio".

Per aumentare la sicurezza generale della rete è stata adottata la politica di utilizzo "minimale" che preclude all'utente l'installazione di applicazioni e la modifica dei principali parametri di configurazione del sistema.

Tale politica va letta principalmente in un'ottica di sicurezza in quanto coadiuvata da altri sistemi di sicurezza (aggiornamenti, sistema di Content-Filtering, antispam, ecc) limita i danni causati da "codici maligni" con cui viene a contatto l'utente.

Elenco sintetico misure adottate

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura adottate
Autenticazione	Accessi non autorizzati	Banche dati	Dominio centralizzato. Proxy Attivazione di dominio UNICO
Antivirus	Perdita dati	Banche dati Informazioni	Software antivirus centralizzato.
Backup	Perdita dati	Banche dati Informazioni	Salvataggio su ogni server
File Server centralizzato	Perdita dati e accessi non autorizzati	Banche dati Informazioni	File Server per gestione centralizzata dei salvataggi
Salvaguardia elettrica	Perdita dati UP-time servers	Banche dati Informazioni	Gruppi continuità
Sistema antincendio	Perdita dati	Banche dati Informazioni	Sistema antincendio Cassetta ignifuga per i backup
Salvaguardia stabili	Accesso ai locali	Banche dati Informazioni	Custodia locali

4.5 Criteri e modalità di ripristino dei dati

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banca di dati trattati.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Banca dati/Data base/Archivio sottoposti a salvataggio:

- AS/400
- I server di rete

Criteri e procedure per il salvataggio e il ripristino dei dati:

Giornalmente:
- Viene eseguito un backup su di un tape con una rotazione di 6 giorni per AS/400 e gli altri server
- Il sistema di backup centralizzato provvede a salvare i dati dal file server e dai database server

Annualmente:
- Viene conservata una cassetta di salvataggio per ogni server

Per il ripristino ci si avvale di strumenti hardware e software legati ai server ed ai software di gestione dei dati.

Pianificazione delle prove di ripristino:
- Trimestrali

4.6 Analisi misure adottate e rischi residui:

	Misure
M001	Autenticazione
M002	Antivirus
M003	Backup
M004	Salvaguardia elettrica
M005	Sistemi antiincendio
M006	Salvaguardia stabili
M007	Formazione specifica
M008	Piano adeguamento sistemi
M009	Firewall
M010	Definizione responsabili accesso ai singoli locali
M012	File server centralizzato

	Evento	Rischio (PXG)	Misura	Rischio Residuo
E001	sottrazione di credenziali di autenticazione	2	M007	1
E002	errore materiale, carenza di consapevolezza, disattenzione o incuria	1	M007	1
E003	comportamenti sleali o fraudolenti	2	M003, M012	0
E004	azione di virus informatici o di programmi suscettibili di recare danno	3	M002 , M009	1
E005	spamming o tecniche di sabotaggio	2	M002, , M009	0
E006	malfunzionamento, indisponibilità o degrado degli strumenti	1	M008	0
E007	accessi esterni non autorizzati	3	M006, M009,	0
E008	intercettazione di informazioni in rete	2	M009, M005	0
E009	ingressi non autorizzati a locali/aree ad accesso ristretto	4	M010	2
E010	sottrazione di strumenti contenenti dati	4	M001; M007, M010	1
E011	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria	2	M005; M003	1
E012	guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)	2	M004;M003	0
E013	errori umani nella gestione	4	M003;M007, M010	1

	della sicurezza fisica			

Attualmente le misure di sicurezza sono sufficienti a soddisfare le misure minime di sicurezza.

Si evidenzia come le misure adottate riescano a ricondurre il rischio entro livelli medi che garantiscono un rispetto della normativa.

Viene posto l'accento a tutti gli incaricati di attenersi alle misure minime di sicurezza indicate anche nell' allegato

Le misure minime richieste relativamente alla gestione di sistemi elettronici saranno pienamente adeguate al disciplinare tecnico definito nell' allegato B del Codice Unico per la Privacy

4.7 Trattamenti senza l'ausilio di strumenti elettronici

In base a quanto stabilito dall'**Art. 30 del Dlgs. n.196 del 30 giugno 2003**, le operazioni di trattamento possono essere effettuate solo da **Incaricati del trattamento** che operano sotto la diretta autorità del **Titolare del trattamento** o, se designato, del **Responsabile di uno specifico trattamento di dati personali**, attenendosi alle istruzioni impartite.

Il **Responsabile di uno specifico trattamento di dati personali** deve predisporre per ogni archivio di cui è responsabile l'elenco degli **Incaricati del trattamento** autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante per l'accesso agli archivi.

In base a quanto stabilito dal **punto 28** del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**, i documenti che contengono dati sensibili o giudiziari debbono essere custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici

In base a quanto stabilito dal **punto 27 e dal punto 28** del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**, **per i trattamenti di dati personali effettuati senza l'ausilio di strumenti** elettronici vengono stabilite le seguenti regole che gli **Incaricati del trattamento** debbono osservare:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.

- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.
- Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

Copie degli atti e dei documenti

In base a quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)**, è fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile del trattamento dei dati personali,** di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile del trattamento dei dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile del trattamento dei dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

Piano Di Adeguamento

Non è stato ancora approvato un piano di adeguamento per dotare TUTTI gli armadi contenenti dati sensibili di una serratura con chiave da affidare ad addetti ben definiti.

E’ stato dato mandato agli uffici di utilizzare gli amadi con chiusura per contenere questo tipo di documenti o vietare l’ingresso ai non autorizzati ai locali contenenti questo tipo di documenti non sufficientemente protetti.
Si dovrà imporre la chiusura a chiave di TUTTI i locali contenenti archivi quando non siano presidiati da personale del Comune.
Eventuale documentazione contenente dati sensibili la cui locazione fisica non preveda armadi chiusi dovrà essere trasportata in altri locali dotati di queste elementari dotazioni di sicurezza e recuperate dagli operatori sono in caso di necessità

E’ auspicabile l’adozione di una banca dati che riepiloghi gli schedari in dotazione degli utenti in maniera da diminuire i rischi di acquisizione errata di documenti.

5. AFFIDAMENTO IN OUTSOURCING

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

In ogni caso, il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali
2. di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali
3. di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come Responsabile del trattamento dei dati, mediante apposito decreto.

Responsabili esterni (outsourcing) del trattamento dei dati per il Comune di Ospedaletto Euganeo

I responsabili esterni sono stati nominati con specifico decreto sindacale.
Il Titolare (per nome del Sindaco in carica) ha nominato le seguenti società responsabili esterni dei trattamenti sotto indicati:

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili, o giudiziari interessati	Soggetto esterno	Descrizione dei criteri per l'adozione delle misure
Pagamenti e riscossioni	Gestione della cassa dell'Ente	Personali	Banca Monte dei Paschi di Siena	L'attività viene svolta a norma di legge come prevede il D.Lgs 30 giugno 2003, n.196
Incasso ruoli e tributi	Gestione dell'incasso ruoli tributi, entrate	Personali	Equitalia Nord SpA (Concessionario delle riscossioni)	L'attività viene svolta a norma di legge come prevede il D.Lgs 30 giugno 2003, n.196 e s.m.i.

Incasso ruoli e tributi	Gestione dell' incasso della tariffa rifiuti	Personali	Consorzio Padova Sud (gestione unificata dei Bacini Padova Tre e Quattro)	L'attività viene svolta a norma di legge come prevede il D.Lgs 30 giugno 2003, n.196
Salvataggio dati	Gestione salvataggio dati server	Personali, sensibili	Icasystems	L'attività viene svolta in base al contratto di manutenzione
Archiviazione sostitutiva	Attività di conservazione	Personali, sensibili	Aruba	L'attività viene svolta in base al contratto di manutenzione e assistenza

6. DICHIARAZIONI D'IMPEGNO

L'originale del presente documento viene custodito presso la sede del Comune, per essere esibito in caso di controlli.

Una sua copia senza gli allegati tecnici verrà consegnata:

- a ciascun responsabile interno del trattamento dei dati personali
- ai responsabili esterni del trattamento dei dati personali
- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali

Gli allegati tecnici potranno essere visionati presso la sede del Comune in accordo con l'ufficio Sistemi Informativi che ne detiene gli originali.