COMUNE DI PONTE SAN NICOLÒ

Provincia di Padova

D.P.S.
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
AGGIORNAMENTO 2007

**Redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g)
del Decreto Legislativo 30 giugno 2003, n. 196,
e del disciplinare tecnico allegato al Decreto sub B).**

Ponte San Nicolò, 30 Marzo 2007

approvato con atto di Giunta Comunale n. 30 del 04.04.2007

Sommario

Tabelle

1 SCOPO DEL DOCUMENTO

Scopo di questo aggiornamento annuale del Documento Programmatico per la Sicurezza nel seguito indicato come D.P.S., è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali effettuato.

L'obbligo di redigere il documento programmatico sulla sicurezza riguarda tutti in casi in cui si trattino dati sensibili o giudiziari con l'utilizzo di strumenti elettronici.

È fissato il termine generale, entro il 31 marzo di ogni anno, per l'aggiornamento periodico di tale documento.

2 AMBITO DI APPLICAZIONE

Il D.P.S. descrive le modalità di gestione delle politiche di sicurezza nel contesto specifico della legge (Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali).

Il D.P.S. riguarda il trattamento dei seguenti dati personali:
- dati personali comuni
- dati sensibili
- dati giudiziari

I dati personali sono trattati con le seguenti modalità:
- con strumentazione elettronica
- senza strumentazione elettronica

3 RIFERIMENTI NORMATIVI

1	Decreto Legislativo 30 giugno 2003, n. 196
2	Disciplinare tecnico, Allegato B) del D.Lgs. 196/2003

4 REVISIONE

Documento	Aggiornamento Documento Programmatico per la Sicurezza		
Versione	2.1	Data Versione	Marzo 2007
Descrizione modifiche	Nessuna		
Causa	AGGIORNAMENTO		

5 CONTENUTI

La redazione del D.P.S. è una "misura minima". Già la precedente disciplina prevedeva l'obbligo di predisporre e aggiornare il D.P.S., almeno annualmente, in caso di trattamento di dati sensibili o relativi a determinati provvedimenti giudiziari effettuato mediante elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico (artt. 22 e 24 Legge 675/1996; art. 6 DPR 318/1999).

Sulla base di quanto prescrive il punto 19. del Disciplinare tecnico, allegato B) al D.Lgs. 196/2003, nel presente documento si forniscono informazioni relative a:

elenco dei trattamenti di dati personali;
individuazione dei tipi di dati personali trattati;
descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
elaborazione della mappa dei trattamenti;
distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
analisi dei rischi che incombono sui dati;
misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

6 DEFINIZIONI

Ai fini del codice si intende per:

"**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

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

"**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

"**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'art. 3, comma 1, lettere da a) a o) e da r) a u), del DPR 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 o di 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 di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

"**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un

servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

"**chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

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

"**rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

"**servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'art. 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

"**abbonato**", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

"**utente**", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

"**dati relativi al traffico**", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

"**dati relativi all'ubicazione**", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

"**servizio a valore aggiunto**", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

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

"**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'art. 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, nonché 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;
"**scopi storici**", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
"**scopi statistici**", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
"**scopi scientifici**", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Secondo l'ISO viene definita la sicurezza un insieme di misure atte a garantire:

disponibilità: l'informazione ed i servizi che eroga devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio;
integrità: l'informazione ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione;
autenticità: garanzia e certificazione della provenienza dei dati;
confidenzialità o **riservatezza**: l'informazione che contiene può essere fruita solo dalle persone autorizzate a compiere tale operazione.

L'approccio complessivo alla sicurezza richiede di considerare aspetti tecnici (sicurezza fisica e logica), strategici (obiettivi e budget), organizzativi (definizione di ruoli, procedure, formazione), economici (analisi dei costi) ed infine giuridici (leggi e raccomandazioni, normative).

7 TITOLARE

Il Titolare del trattamento è:

Comune di Ponte San Nicolò (Padova)			
CAP	35020	Indirizzo	Viale del Lavoro n. 1
Telefono			049 8968611

8 ORGANIZZAZIONE DEL COMUNE

Si riassume nella tavola che segue l'organigramma della distribuzione delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati e della sicurezza.

Nome	**Qualifica**	**Servizio/attività di competenza**
NIEDDU Mariano	Segretario/Direttore Generale	Servizio Gestione Risorse Umane; Servizio Controlli Interni, Attività di assistenza agli Organi Istituzionali
BARZON Nicoletta	Vicesegretaria, Capo Settore Affari Generali, Responsabile Sistema di Gestione per la Qualità	Settore Affari Generali; Servizio Sistema di Gestione per la Qualità
Questori Lucio	Capo Settore Servizi Finanziari	Settore Servizi Finanziari
BETTIO Roberto	Capo Settore Uso e Assetto del Territorio	Settore Uso e Assetto del Territorio
CEOLA Lorenzo	Capo Settore Lavori Pubblici	Settore Lavori Pubblici e Ambiente
INFANTE Laura	Capo Settore Servizi alla Persona	Settore Servizi alla Persona
MARITAN Giorgio	Capo Servizio Informatizzazione	Sicurezza Informatica
BARBIERI Antonio	Capo Servizio Polizia Locale	Attività di Polizia Giudiziaria

9 IL TITOLARE DEL TRATTAMENTO, I RESPONSABILI, GLI INCARICATI

9.1 Compiti del Titolare

In base a quanto definito dall'art. 4, punto 1, lett. f) del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) 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 (D.Lgs. 196/2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. 196/2003) tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

In base a quanto stabilito dall'art. 29 del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003), 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 ed 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 (D.Lgs. 196/2003) 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 (D.Lgs. 196/2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. 196/2003).

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 (D.Lgs. 196/2003) 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.

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

9.2 Compiti del responsabile di uno specifico trattamento di dati personali

In base a quanto stabilito dall'art. 29 del Codice in materia di protezione dei dati personali (D.Lgs. 196/2003), il Titolare del trattamento, ove necessario, per esigenze organizzative,può designare facoltativamente uno o più soggetti Responsabili del trattamento.

Il Responsabile di uno specifico trattamento di dati personali è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo al quale il Titolare del trattamento affida il compito di gestire il trattamento dei dati personali di una o più Banche di dati ed ha il compito di individuare, nominare e incaricare per iscritto, gli incaricati del trattamento dei dati personali del trattamento specifico di cui gli è stata assegnata la responsabilità.

I Responsabili di uno specifico trattamento di dati personali 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 di uno specifico trattamento di dati personali ha i seguenti compiti fondamentali:

Nominare gli Incaricati del trattamento dei dati personali limitatamente alle Banche di dati di cui sono responsabili;
Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.Lgs. 196/2003);
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.

La nomina del Responsabile di uno specifico trattamento di dati personali può essere revocata in qualsiasi momento dal Titolare.

9.3 Mansionari

Per il trattamento dei dati personali, il Titolare ha nominato i responsabili già indicati che a loro volta provvedono nell'ambito della verifica annuale degli ambiti del trattamento a designare o aggiornare le precedenti designazioni di incaricati al trattamento.

Il trattamento dei dati personali viene effettuato solo dai soggetti che hanno ricevuto un formale incarico, mediante documentata preposizione di ogni persona ad una unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima o, in taluni casi, designazione per iscritto di un singolo incaricato, con la quale si individua l'ambito del trattamento consentito.

9.3.1 Mansionario dei Responsabili del trattamento

Ai responsabili al trattamento dei dati sono attribuiti incarichi formali di ordine organizzativo e direttivo con i seguenti compiti.

A) Trattamento dei dati personali

verificare che i trattamenti in corso o da intraprendere presso il settore siano rispondenti a quanto disposto dal nuovo codice e ove difformi dalla norma, il trattamento deve essere adeguato o cessare

B) Banche dati:

provvedere ad un censimento delle banche dati presenti nel proprio settore,aggiornare, ad ogni variazione intervenuta, le informazioni sulle banche dati;
individuare i soggetti abilitati all'accesso alle risorse di rete protette, in relazione ai compiti svolti dal personale;
verificare - d'intesa con il Responsabile della Sicurezza - che la configurazione e l'utilizzo delle risorse presenti siano conformi a quanto stabilito nel Piano operativo di consolidamento del sistema informatico al fine di garantire la riservatezza e l'accesso selezionato alle banche dati contenenti dati personali; la verifica può essere effettuata sulla base delle informazioni che deve comunicare l'amministratore di sistema sulla composizione dei gruppi di utenti e sulle restrizioni di accesso assegnate alle cartelle di lavoro sul server;
prevedere procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
prevedere procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati;
nomina degli incaricati del trattamento di dati personali e sensibili;
provvedere alla nomina degli incaricati di ciascun trattamento mediante atto formale di incarico
provvedere all'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati sia nel caso di trattamenti effettuati con strumenti elettronici che nel caso di trattamenti effettuati senza strumenti elettronici.

C) osservanza delle misure di sicurezza

garantire che il trattamento, la comunicazione e la diffusione dei dati avvenga nel rispetto delle vigenti disposizioni, ivi comprese quelle relative alla sicurezza;
segnalare al Responsabile della Sicurezza le necessità di acquisizione o di adeguamento delle dotazioni del settore al fine del rispetto delle disposizioni in materia di sicurezza dei dati personali;
segnalare al titolare del trattamento i nuovi trattamenti di dati personali o la modifica negli elementi essenziali dei trattamenti in atto, al fine dell'eventuale preventiva notificazione al Garante.

9.3.2 Mansionario del Responsabile della Sicurezza

Il responsabile per la sicurezza: alla posizione sono assegnati i seguenti compiti:

progettare, realizzare e mantenere misure di sicurezza tali da soddisfare le linee strategiche di indirizzo definite dal Titolare;
definire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi, delle procedure e dei sistemi informatici esistenti;
definire un'architettura di sicurezza, che soddisfi i requisiti di cui sopra, con particolare riferimento alla armonizzazione delle misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione;
curare progettazione e realizzazione del sistema di sicurezza, sulla base degli elementi da proteggere e delle minacce cui detti elementi sono sottoposti;
definire ed attuare piani e strumenti di monitoraggio continuo della sicurezza;
aggiornare periodicamente il sistema di sicurezza per renderlo sempre adeguato alle nuove minacce;
mantenere il sistema di sicurezza informatica, per assicurarne costante efficienza e disponibilità;
fornire supporto alla formazione del personale del Comune in tema di sicurezza informatica;
emanare procedure interne inerenti la sicurezza che regolino gli accessi agli archivi ed ai sistemi informativi e fissino norme operative di utilizzo e gestione dei sistemi;
gestire opportunamente il sistema di autenticazione ed autorizzazione;
realizzare e mantenere aggiornati i sistemi antintrusione ed antivirus;
provvedere affinché siano regolarmente effettuate tutte le operazioni periodiche di sicurezza dei dati e dei sistemi e quelle tese ad assicurare la disponibilità dei dati e dei sistemi;
provvedere al controllo delle misure di prevenzione degli accessi abusivi di cui l'art. 615 ter del C.P.;
provvedere in modo che sia predisposto, ed aggiornato con cadenza annuale ed entro e non oltre la data del 31 marzo, il documento programmatico sulla sicurezza dei dati previsto dall'art. 34, comma 1, lettera g) del D.Lgs. 196/2003;
effettuare le verifiche periodiche dell'ambiente tecnologico e della situazione delle banche dati contenenti dati personali e particolari;
disporre in modo che il software utilizzato sia originale e adeguatamente licenziato e che, ove previsto, ne vengano correttamente effettuati gli aggiornamenti;
disporre in modo che l'accesso ai locali dei server sia controllato;
custodire la copia delle credenziali informatiche laddove l'accesso è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione;
ogni altro adempimento che la normativa prevede tenuto anche conto delle sue evoluzioni o successive modifiche come disposto dall'art. 36 del Codice.

Per tutte le attività predette il Responsabile della Sicurezza può avvalersi di risorse esterne (fornitori/consulenti specialisti in sicurezza)

9.3.3 Mansionario per Incaricati al trattamento

Il responsabile designa gli incaricati con una determinazione basata sul seguente schema:

"Il personale assegnato all'Unità Organizzativa è ritenuto formalmente incaricato al trattamento dei dati strettamente necessari per l'adempimento dei compiti assegnati ed altresì all'accesso per effettuare operazioni di trattamento ai seguenti dati particolari e in particolare per le seguenti finalità:

Gestione ……..	Tutti i trattamenti di cui l'art. 4 D.Lgs. 196/2003
Gestione ……..	
Gestione ……..	
Gestione ……..	
Gestione ……..	
Gestione ……..	

Definizioni

"dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
"**dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;
"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'art. 3, comma 1, lettere da a) a o) e da r) a u), del DPR 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 o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
"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 di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Il trattamento dei dati che saranno svolti

Il "trattamento" che Lei effettuerà è qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti:

la raccolta;
la registrazione cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
l'organizzazione;
la conservazione;
la consultazione;
l'elaborazione;
la modificazione;
la selezione;
l'estrazione;
il raffronto;
l'utilizzo;
l'interconnessione ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
il blocco ovvero la conservazione dei dati con sospensione temporanea di ogni altra operazione di trattamento;
la comunicazione cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
la diffusione cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
la cancellazione e distruzione di dati.

Prescrizioni generali su come deve avvenire il trattamento dei dati

I dati personali oggetto di trattamento devono essere:

trattati in modo lecito e secondo correttezza;
raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, ed in ogni caso nei limiti in cui il trattamento sia necessario per il funzionamento della nostra organizzazione;
esatti e, se necessario, aggiornati;
pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Sarà Sua cura effettuare le operazioni di trattamento, che Le vengono affidate, nel rispetto delle disposizioni di legge, verificando in particolare che ai soggetti interessati sia stata data l'informativa.

Descrizione degli incarichi

In relazione alle mansioni lavorative, viene dato l'incarico di trattare i seguenti dati personali*:*

dati di natura comune, che consistono in informazioni di carattere anagrafico ed in altre notizie il cui trattamento è necessario in relazione ai procedimenti amministrativi di competenza del settore di appartenenza;

eventuali dati di natura sensibile o giudiziaria che consistono in informazioni e altre notizie il cui trattamento è necessario in relazione ai procedimenti amministrativi di competenza del settore di appartenenza.

Disposizioni per il trattamento dei dati personali

Per le attività connesse, ci si dovrà attenere alle seguenti disposizioni:

utilizzare direttamente le credenziali personali assegnate per accedere alle procedure informatiche;
non modificare la configurazione della propria postazione apparecchiatura informatica;
procedere all'aggiornamento dei dati su richiesta degli interessati o comunque quando a conoscenza della variazione;
non consentire l'accesso a terzi alla propria apparecchiatura informatica con le proprie credenziali di autenticazione;
è fatto obbligo di adottare le necessarie cautele per assicurare la segretezza delle credenziali assegnate. La perdita o la venuta a conoscenza di utilizzo da parte di altri delle proprie credenziali deve essere comunicata al responsabile della Sicurezza il quale provvederà al rilascio di nuove e sostitutive modalità di autenticazione al sistema informatico;
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. A tale fine, l'incaricato, al momento dell'attribuzione della password, scrive la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa, sigillata riportando all'esterno della stessa il nominativo dell'incaricato. L'incaricato ha facoltà di nominare un altro dipendente dell'ente ai fini dell'accesso alla postazione e per l'eventuale accesso alla posta elettronica ed internet, indicando il suo nominativo all'esterno della busta. La busta deve essere controfirmata nei lembi di chiusura, con firma anche del fiduciario e consegnata a chi custodisce le copie delle password;
dell'eventuale accesso, in caso di assenza, verrà data tempestiva comunicazione all'incaricato e si provvederà a sostituire ed assegnare un nuova parola chiave;
è fatto obbligo a NON lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
verificare la presenza attiva del sistema antivirus;
comunicare al Responsabile per la Sicurezza designato il mancato utilizzo di una password per oltre sei mesi al fine di disattivarla;
non installare alcuna applicazione informatica o programma non autorizzati dal Responsabile della Sicurezza e dal Responsabile al Trattamento;
i supporti removibili, Floppy Disk, CD-ROM, ZIP, Nastri ecc, 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, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi e 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;
in caso di trattamento di dati su formato cartaceo, questi dovranno essere conservati nelle attrezzature d'ufficio presenti. Incartamenti contenenti dati sensibili non devono essere lasciati incustoditi sulle scrivanie o altro luogo non chiuso anche durante l'orario d'ufficio. Al termine dell'orario d'ufficio essi devono essere custoditi nelle strutture d'ufficio dotate di serratura e regolarmente chiuse;

l'accesso agli archivi deve essere controllato e registrati i soggetti ad essi ammessi dopo l'orario di chiusura degli uffici;
è ammesso l'accesso ai soli dati personali la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione;
in caso di installazione di nuovi dati, programmi ecc sul proprio personal computer è obbligatorio che i supporti che li contengono siano preventivamente controllati dal sistema antivirus".

9.3.4 Verifiche

In forza degli art. 34 e 35 della legge, disciplinanti le misure minime di sicurezza, l'individuazione dell'ambito del trattamento consentito, è soggetto ad aggiornamento periodico con cadenza annuale, sia per i trattamenti effettuati con strumenti elettronici che per quelli che avvengono senza l'ausilio di tali strumenti.

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.

9.3.5 Altro

Per i casi di affidamento del trattamento dei dati personali ad altri soggetti esterni all'Ente si procede con atto di Nomina di Responsabile da parte del Titolare.

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.

10 TRATTAMENTI DEI DATI PERSONALI

In questa sezione si applica la regola 19.1 dell'Allegato tecnico. Al fine di classificare i trattamenti dei dati posti in essere dal Titolare.
Si procede come segue:
• sono individuati i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili) ed alla categoria di soggetti cui essi si riferiscono (utenti, fornitori, personale, ...);
• sono descritti gli strumenti con i quali si effettuano i trattamenti.

10.1 Tipologie di dati trattati

Il trattamento dei dati sensibili e giudiziari è effettuato perché autorizzato da disposizioni normative e regolamentari nelle quali sono specificati i tipi di dati che possono essere trattati e le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

L'atto di natura regolamentare che specifica le finalità di rilevante interesse pubblico e i tipi di dati sensibili e giudiziari, le operazioni eseguibili, nonché i limiti della comunicazione degli stessi ad altri soggetti pubblici di cui all'art. 20 è stato regolarmente approvato.

Nel seguito alcune indicazioni di merito sulla classificazione dei dati facendo riferimento ai documenti di linee guida emanate dalle autorità nazionali relativamente ad: accesso, comunicazione, diffusione di dati pubblici.

I dati, quando siano memorizzati ed elaborati sia con strumentazione elettronica che con strumentazione diversa da quella elettronica assumono forme diverse:

• dati strutturati aventi formato ammesso nei campi ed archivi di una base di dati;
• documenti, ovvero dati non strutturati, caratterizzati dall'essere espressi in linguaggio naturale.

Una ulteriore classificazione è la seguente:

• dati accessibili pubblicamente: questa definizione fa riferimento all'assenza di requisiti di riservatezza, e riflette quindi un aspetto legato alla legittimità della consultazione da parte di soggetti comunque interessati. Risulta quindi applicabile ad un sottoinsieme dei dati detenuti dai soggetti pubblici (ad esempio i provvedimenti);
• dati detenuti da un soggetto pubblico: fa riferimento alla natura pubblica del titolare del trattamento (ad esempio: dati anagrafici di persone fisiche e giuridiche) che può eventualmente esserne anche il produttore;
• dati di interesse di un soggetto pubblico: fa riferimento alla natura pubblica del fruitore nell'interesse della collettività e riguarda informazioni che devono essere in determinate condizioni rese accessibili ai soggetti pubblici per il perseguimento di fini istituzionali.

La conoscibilità dei dati pubblici può essere consentita attraverso tre diverse modalità di scambio, a seconda dei ruoli che assumono l'amministrazione che detiene i dati e il soggetto che intende conoscerli:

- l'accesso è di iniziativa del soggetto interessato e gli permette di esprimere le sue esigenze;
- la comunicazione è di iniziativa dell'amministrazione oppure dell'interessato che ne ha fatto richiesta e consiste nel far pervenire i dati ad uno o più destinatari predeterminati;
- la diffusione è di iniziativa della amministrazione e consiste nel rendere i dati disponibili ad una platea indeterminata di soggetti anche tramite pubblicazione, tradizionale o su internet; il grado di effettiva disponibilità dipende dalle modalità prescelte.

Si possono avere quattro situazioni distinte per quanto concerne la conoscibilità dei dati detenuti da soggetti pubblici:

- dati conoscibili da chiunque;
- dati *a conoscibilità circoscritta* riservata ad alcuni soggetti pubblici, oppure ad alcune categorie professionali o ad altre particolari categorie di soggetti;
- dati in atti e documenti *conoscibili* ai sensi della Legge 7 agosto 1990, n. 241 da parte di chi ha un interesse personale e concreto e per la tutela di situazioni giuridicamente rilevanti;
- dati *conoscibili dal solo soggetto pubblico* che li detiene, coperti cioè dal segreto d'ufficio o dal segreto statistico o sottoposti a particolare tutela dal D.Lgs. 196/2003.

Nei casi di trattamento, comunicazione e diffusione, si deve provvedere ad assicurare la riservatezza e l'integrità dei dati trasmessi. In generale:

- se le informazioni devono essere trasmesse in maniera tale che il solo destinatario possa conoscerle, è necessario ricorrere a tecniche in grado di assicurarne la riservatezza;
- se è necessario garantire aspetti di integrità alle informazioni, devono essere previste tecniche in grado di assicurare la non modificabilità delle informazioni durante la trasmissione;
- se è necessario assicurare da parte del mittente requisiti di autenticazione, utili anche per il non ripudio, occorre prevedere meccanismi di trattamento del documento o del dato che li garantiscano (vedi firma digitale);
- se è necessario assicurare al mittente il non ripudio da parte del destinatario, occorre prevedere meccanismi di notifica di ricezione (posta elettronica certificata).

Requisiti per la comunicazione:

Tipologie di dati	**Non ripudio**	**Integrità**	**Riservatezza**	**Autenticazione**
Conoscibili da chiunque	**N**	**N**	**N**	**N**
A conoscibilità circoscritta ad alcuni soggetti pubblici	**S**	**S**	**N**	**N**
Accessibili soltanto al soggetto pubblico che li detiene a loro volta categorizzati in dati Personali e/o Sensibili e/o Giudiziari	**S**	**S**	**S**	**S**

Tabella 1 – Requisiti per la comunicazione

10.2 Natura dei dati

Nell'ambito del presente documento, i **tipi di dati** sono codificati come segue:

Tipo	Descrizione
P	Personali
S	Sensibili
G	Giudiziari

Tabella 2 – Natura dei dati

Per quanto riguarda i Trattamenti specificatamente classificati quali:

- trattamenti in ambito pubblico
- trattamenti con finalità di rilevante interesse pubblico

il Comune fa riferimento agli articoli del Codice e in particolare come nel seguito indicati.

10.2.1 Trattamenti in ambito pubblico (D.Lgs. 196/2003)

10.2.1.1 Art. 59 (Accesso a documenti amministrativi)

Fatto salvo quanto previsto dall'art. 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla Legge 7 agosto 1990, n. 241 e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

10.2.1.2 Art. 60 (Dati idonei a rivelare lo stato di salute e la vita sessuale)

Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

10.2.2 Finalità di rilevante interesse pubblico (D.Lgs. 196/2003)

10.2.2.1 Art. 62 (Dati sensibili e giudiziari)

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative alla tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché al rilascio di documenti di riconoscimento o al cambiamento delle generalità.

10.2.2.2 Art. 63 (Consultazione di atti)

1. Gli atti dello stato civile conservati negli Archivi di Stato sono consultabili nei limiti previsti dall'art. 107 del D.Lgs. 29 ottobre 1999, n. 490.

10.2.2.3 Art. 64 (Cittadinanza, immigrazione e condizione dello straniero)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e del profugo e sullo stato di rifugiato.
Nell'ambito delle finalità di cui al comma 1 è ammesso, in particolare, il trattamento dei dati sensibili e giudiziari indispensabili:

a) al rilascio e al rinnovo di visti, permessi, attestazioni, autorizzazioni e documenti anche sanitari;

b) al riconoscimento del diritto di asilo o dello stato di rifugiato, o all'applicazione della protezione temporanea e di altri istituti o misure di carattere umanitario, ovvero all'attuazione di obblighi di legge in materia di politiche migratorie;

c) in relazione agli obblighi dei datori di lavoro e dei lavoratori, ai ricongiungimenti, all'applicazione delle norme vigenti in materia di istruzione e di alloggio, alla partecipazione alla vita pubblica e all'integrazione sociale.

Il presente articolo non si applica ai trattamenti di dati sensibili e giudiziari effettuati in esecuzione degli accordi e convenzioni di cui all'art. 154, comma 2, lettere a) e b), o comunque effettuati per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad espressa disposizione di legge che prevede specificamente il trattamento.

10.2.2.4 Art. 65 (Diritti politici e pubblicità dell'attività di organi)

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di:

a) elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari;

b) documentazione dell'attività istituzionale di organi pubblici.

2. I trattamenti dei dati sensibili e giudiziari per le finalità di cui al comma 1 sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti:

a) lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità;

b) le richieste di referendum, le relative consultazioni e la verifica delle relative regolarità;

c) l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi;

d) l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni di inchiesta, il rapporto con gruppi politici;

e) la designazione e la nomina di rappresentanti in commissioni, enti e uffici.

3. Ai fini del presente articolo, è consentita la diffusione dei dati sensibili e giudiziari per le finalità di cui al comma 1, lettera a), in particolare con riguardo alle sottoscrizioni di liste, alla presentazione delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti.

4. Ai fini del presente articolo, in particolare, è consentito il trattamento di dati sensibili e giudiziari indispensabili:

a) per la redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

b) per l'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo.

5. I dati sensibili e giudiziari trattati per le finalità di cui al comma 1 possono essere comunicati e diffusi nelle forme previste dai rispettivi ordinamenti. Non è comunque consentita la divulgazione dei dati sensibili e giudiziari che non risultano indispensabili per assicurare il rispetto del principio di pubblicità dell'attività istituzionale, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

10.2.2.5 Art. 66 (Materia tributaria e doganale)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dei soggetti pubblici dirette all' applicazione, anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonché in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane.

Si considerano inoltre di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi e alla adozione dei provvedimenti previsti da leggi, regolamenti o dalla normativa comunitaria, nonché al controllo e alla esecuzione forzata dell'esatto adempimento di tali obblighi, alla effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari.

10.2.2.6 Art. 67 (Attività di controllo e ispettive)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di:

a) verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti;

b) accertamento, nei limiti delle finalità istituzionali, con riferimento a dati sensibili e giudiziari relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'art. 65, comma 4.

10.2.2.7 Art. 68 (Benefici economici ed abilitazioni)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.

Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione:

a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia;

b) alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive;

c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti;

d) al riconoscimento di benefici connessi all'invalidità civile;

e) alla concessione di contributi in materia di formazione professionale;

f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;
g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.

Il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la trasparenza delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

10.2.2.8 Art. 69 (Onorificenze, ricompense e riconoscimenti)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali.

10.2.2.9 Art. 70 (Volontariato e obiezione di coscienza)

Si considerano di rilevante interesse pubblico, ai sensi dell'articolo 20 e 21, le finalità di applicazione della disciplina in materia di rapporti tra i soggetti pubblici e le organizzazioni di volontariato, in particolare per quanto riguarda l'elargizione di contributi finalizzati al loro sostegno, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale.

Si considerano, altresì, di rilevante interesse pubblico le finalità di applicazione della legge 8 luglio 1998, n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza.

10.2.2.10 Art. 71 (Attività sanzionatorie e di tutela)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità:
a) di applicazione delle norme in materia di sanzioni amministrative e ricorsi;
b) volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo, anche ai sensi dell'articolo 391-quater del codice di procedura penale, o direttamente connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo o di un'ingiusta restrizione della libertà personale.

Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se il diritto da far valere o difendere, di cui alla lettera b) del comma 1, è di rango almeno pari a quello dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

10.2.2.11 Art. 72 (Rapporti con enti di culto)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative allo svolgimento dei rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose.

10.2.2.12 Art. 73 (Altre finalità in ambito amministrativo e sociale)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali, con particolare riferimento a:

a) interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;

b) interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;

c) assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;

d) indagini psico-sociali relative a provvedimenti di adozione anche internazionale;

e) compiti di vigilanza per affidamenti temporanei;

f) iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;

g) interventi in tema di barriere architettoniche.

Si considerano, altresì, di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità:

a) di gestione di asili nido;

b) concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico;

c) ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;

d) di assegnazione di alloggi di edilizia residenziale pubblica;

e) relative alla leva militare;

f) di polizia amministrativa anche locale, salvo quanto previsto dall'art. 53, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo;

g) degli uffici per le relazioni con il pubblico;

h) in materia di protezione civile;

i) di supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;

l) dei difensori civici regionali e locali.

10.2.2.13 Art. 112 (Finalità di rilevante interesse pubblico)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli effettuati al fine di:

a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette; b) garantire le pari opportunità;

c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;

d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;
e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;
f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del Decreto Legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente;
g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;
h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;
i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;
l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;
m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;
n) svolgere l'attività di indagine e ispezione presso soggetti pubblici;
o) valutare la qualità dei servizi resi e dei risultati conseguiti.

La diffusione dei dati di cui alle lettere m), n) ed o) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

10.2.3 Trattamento per scopi storici (D.Lgs. 196/2003)

10.2.3.1 Art. 98 (Finalità di rilevante interesse pubblico)

Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative ai trattamenti effettuati da soggetti pubblici:
a) per scopi storici, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato e negli archivi storici degli enti pubblici, secondo quanto disposto dal Decreto Legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice;
b) che fanno parte del sistema statistico nazionale (Sistan) ai sensi del Decreto Legislativo 6 settembre 1989, n. 322, e successive modificazioni;
c) per scopi scientifici.

10.2.3.2 Art. 99 (Compatibilità tra scopi e durata del trattamento)

Il trattamento di dati personali effettuato per scopi storici, statistici o scientifici è considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.
Il trattamento di dati personali per scopi storici, statistici o scientifici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati. Per scopi storici, statistici o scientifici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento.

10.2.3.3 Art. 100 (Dati relativi ad attività di studio e ricerca)

Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli sensibili o giudiziari. Resta fermo il diritto dell'interessato di opporsi per motivi legittimi ai sensi dell'art. 7, comma 4, lett. a).I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della Legge 7 agosto 1990, n. 241. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

10.2.3.4 Art. 101 (Modalità di trattamento)

I dati personali raccolti per scopi storici non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'art. 11. I documenti contenenti dati personali, trattati per scopi storici, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.
I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

10.2.4 Normativa di riferimento per le principali finalità di rilevante interesse pubblico

Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Codice civile (artt. 2094-2134); legge 20.05.1970, n. 300; legge 12.03.1999, n. 68; legge 8.03.2000, n. 53; d.lgs. 18.08.2000, n. 267; d.lgs. 30.03.2001, n. 165; d.P.R. 29.10.2001, n. 461; CCNL; Contratto collettivo decentrato di ogni singolo ente; Regolamenti comunali
Servizi demografici/Anagrafe - Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero, Stato Civile, Elettorale, Leva Militare	Codice civile (artt. 43-47); legge 24.12.1954, n. 1228; d.P.R. 30.05.1989, n. 223; d.P.R. 6.09.1998, n. 323 Tenuta delle anagrafi della popolazione residente in Italia e di cittadini italiani residenti all'estero (art. 62, d.lgs. 196/2003) Codice civile (artt. 84 e ss.; artt. 106 e ss.); d.P.R. 3.11.2000, n. 396 d.P.R. 20.03.1967, n. 223 Legge 8.07.1998, n. 230
Polizia municipale - Attività relativa all'infortunistica stradale Gestione delle procedure sanzionatorie Attività di polizia annonaria, commerciale e amministrativa Trattamenti sanitari	d.Lgs. 30.04.1992, n. 285 e successive modifiche e integrazioni (C.D. artt. 11-12); d.P.R. 16.12.1992, n. 495 (regolamento di esecuzione e di attuazione del Codice della Strada) Attività di polizia amministrativa (art. 73, comma 2, lett. f), d.lgs. 196/2003) R.d. 27.07.1934, n. 1265 (art. 358); legge 24.11.1981, n. 689; d.lgs. 30.04.1992, n. 285 (Codice della strada, art. 116); d.P.R. 16.12.1992, n. 495 (Regolamento di esecuzione e di attuazione del nuovo Codice della strada); d.lgs. 18.08.2000, n. 267; (art. 71, comma 1, d.lgs. 196/2003) R.d. 18.06.1931, n. 773 (artt. 5 e 75); legge 28.03.1991, n. 112; legge 25.08.1991, n. 28; d.lgs. 31.03.1998, n. 114; d.P.R. 30.4.1999, n. 162; d.P.R. 26.10.2001, n. 430; regolamenti comunali Legge 13.05.1978, n. 180 e successive modifiche e integrazioni; legge 23.12.1978, n. 833
Gestione procedimenti e documenti, Protocollo	d.P.R. 445/2000
Servizi sociali	Codice civile (art. 403); d.P.R. 24.07.1977, n. 616; legge 4.05.1983, n. 184; legge 8.11.2000, n. 328; legge 28.03.2001, n. 149 Legge 13.05.1978, n. 180 e successive modifiche e integrazioni; legge 23.12.1978, n. 833 Legge 5.02.1992, n. 104; legge 8.11.2000, n. 328 Legge 28.08.1997, n. 285; legge 8.11.2000, n. 328; Legge 5.12.1992, n. 104; d.lgs. 31.03.1998, n. 112 e relative disposizioni di attuazione; d.lgs. 18.08.2000, n. 267; legge 3.04.2001, n. 119; leggi regionali

Tabella 3 – Fonti normative finalità di rilevante interesse pubblico

10.2.5 Comunicazione e diffusione dei dati

Nelle tavole che seguono un elenco, non esaustivo, delle possibili comunicazioni che avvengono normalmente, in presenza del servizio, tra il COMUNE e le strutture territoriali esterne locali e centrali.

Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	a) alle organizzazioni sindacali b) agli enti assistenziali e previdenziali agli enti assicurativi; c) alla Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive, ai sensi della legge n. 662/1996, in merito agli incarichi conferiti dal Comune o da altri soggetti a dipendenti; d) alle amministrazioni provinciali ed al Centro regionale per l'impiego, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette"; e) agli uffici giudiziari: su richiesta dati di singoli dipendenti riferiti ad indagini f) Ministero Finanze
Servizi demografici/Anagrafe Gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero, Stato Civile, Elettorale, Leva Militare	a) Procure della Repubblica; Questura; Forze di polizia; INPS; Ministero del Tesoro; società esazione ; Ministero dell'Interno b) ricercatori (in relazione a particolari ricerche o indagini storiche); c) ASL; d) altri Comuni; e) agli uffici giudiziari f) alla Commissione elettorale circondariale; g) alla Procura; h) alla Prefettura per le finalità elettorali; i) ai sensi dell'art. 51 del DPR 20 marzo 1967, n. 223, come modificato dall'art. 177, comma 5, del d.lgs. 196/2003, le liste elettorali possono essere inoltre rilasciate in copia per le finalità connesse all' applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso j) al distretto militare di appartenenza dell'obiettore; k) alla Presidenza del Consiglio dei Ministri l) soggetti esterni autorizzati ad inglobare gli obiettori di coscienza nel proprio organico
Polizia municipale - Attività relativa all'infortunistica stradale Gestione delle procedure sanzionatorie Attività di polizia annonaria, commerciale e amministrativa Trattamenti sanitari	a) Motorizzazione civile; b) Prefettura c) altri Comuni d) Agenzia del territorio, CCIAA e) Autorità giudiziaria, autorità di pubblica sicurezza f) A.S.L.

Tabella 4 – Comunicazione e diffusione

10.3 Modalità del trattamento

I trattamenti effettuati sono quelli definiti nel Codice e precisamente: "tutte le operazioni o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

In particolare per quanto riguarda la raccolta e l'elaborazione viene identificata la seguente sottoclassificazione:

1	Organizzazione ed elaborazione in banche dati non prevalentemente automatizzate;
2	Raccolta dati presso l'interessato;
3	Raccolta dati presso registri, elenchi, atti o documenti pubblici;
4	Raccolta dati presso terzi;
6	Organizzazione ed elaborazione in banche dati automatizzate.

Tabella 5 – Modalità trattamento

10.4 Strumenti per il trattamento dei dati

La classificazione articolata degli strumenti è riportata nella tavola che segue:

A	Archivi, schedari, fascicoli cartacei;
B	Elaboratori non in rete;
C	Postazioni di lavoro in rete locale;
D	Postazioni di lavoro in rete pubblica;
E	Server farm;
F	Videosorveglianza o altri sistemi di rilevazione delle immagini;
G	Altro.

Tabella 6 – Strumenti

10.4.1 Schedari ed altri supporti cartacei (trattamento senza l'ausilio di strumenti elettronici)

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

Gli Archivi sono localizzati presso le rispettive aree organizzative e presso l'Archivio generale.

10.4.2 Elaboratori (trattamento con l'ausilio di strumenti elettronici)

Il trattamento dei dati personali viene effettuato con strumentazione elettronica costituita da una architettura di rete interconnessa tra il sistema centrale e tutte le postazioni di lavoro. La tecnologia di riferimento è basata sullo stato dell'arte maturo e consolidato dei sistemi operativi desktop. I sistemi operativi non supportati od obsoleti rientrano in piani di reintegro.

10.5 Distribuzione delle aree, locali e strumenti con cui si effettuano i trattamenti

Comune di Ponte San Nicolò (Padova)			
CAP	35020	Indirizzo	Sede Municipale – Viale del Lavoro, 1
Telefono	049 8968611		

Comune di Ponte San Nicolò (Padova)			
CAP	35020	Indirizzo	Biblioteca – Via Aldo Moro, 28
Telefono	049 8961532		

10.6 Categorie di interessati

Gli interessati del trattamento sono sintetizzati nella seguente tabella

1	Personale Dipendente
2	Contribuenti
3	Residenti
4	Non residenti
5	Attività Economiche

10.7 Finalità delle banche dati

Le finalità dei trattamenti mediante strumenti elettronici sui dati personali organizzati in banche dati sono solo quelle istituzionali. Le Comunicazioni sono solo quelle previste per legge o regolamento o verso responsabili appositamente nominati. Le Diffusioni sono solo quelle previste per legge e regolamento.

10.7.1 Sistemi informativi automatizzati

Rispetto alle ultime rilevazioni sono state eseguite le normali operazioni di manutenzione evolutiva

10.7.2 Strumenti software di produttività individuale

Si tratta degli strumenti di produttività individuale. Viene adottata la suite Office del produttore Microsoft.
Con questi strumenti, parte delle banche dati generate sono e rimangono ricoverate nelle postazioni di lavoro in cui vengono trattate.

10.7.3 Banche dati principali trattate con strumentazione elettronica

10.7.3.1 Sistema informativo

Dalle banche dati del sistema informativo centrale sono derivate banche dati cartacee che sono trattate dagli incaricati
Tutte le banche dati sono inserite nelle procedure di sicurezza. Il rischio relativo a riduzione di disponibilità e perdita di integrità è basso.

10.7.3.2 Banche dati residenti sulle postazioni di lavoro

Delle banche dati esistenti, generate con applicazioni di produttività individuale, esiste il corrispondente su supporto cartaceo e sul quale viene effettuato il trattamento da parte degli incaricati. La natura dei dati personali include anche quelli definiti come sensibili e giudiziari.
L'organizzazione dell'architettura del sistema informativo prevede, quale regola interna che le banche dati siano immediatamente riversate sui sistemi server al fine di essere inserite nelle procedure di sicurezza.
La sincronizzazione degli elementi banche dati in formato documenti, prodotti con la suite di produttività individuale di Microsoft, o con strumenti di reportistica propri del sistema informativo è gestita direttamente e manualmente dall'utente operatore. La possibilità di garantire l'immediato e trasparente riversamento sul server dipende da una specifica configurazione del profilo utente.

10.7.3.3 Sintesi e Riepilogo Banche dati

FUNZIONE	**BANCHE DATI DI RIFERIMENTO**	**DATI PERSONALI (C=comuni S=sensibili)**		**STRUMENTO (M=elettronico C=cartaceo)**	
Contabilità, Bilancio	Bilancio Professionisti,Economato Contabilità finanziaria , Inventario	C	S	M	C
Protocollo	Protocollo generale	C	S	M	C
Risorse Umane e Rilevazione Presenze	Gestione procedimento economico giuridico Risorse Umane; Rilevazione delle presenze e delle assenze	C	S	M	C
Segreteria e Affari generali	Procedimenti amministrativi di competenza, provvedimenti, contratti, affari generali	C	S	M	C
Tributi	Gestione ICI	C	S	M	C
SS.DD.	Anagrafe,Elettorale, Stato Civile,Leva	C	S	M	C
Territorio	Pratiche edilizie	C	S	M	C
Polizia Locale	Codice della strada	C	S	M	C

10.7.3.4 Altre Banche dati

Altre banche dati sia su postazioni elettroniche che su registri e supporti cartacei archiviati sulle quali viene effettuato il trattamento da parte degli incaricati. La natura dei dati personali include anche quelli definiti come sensibili e giudiziari. I dati fascicolati sono custoditi. La situazione è come già rilevato nelle precedenti versioni della presente edizione del D.P.S.

Finalità	**Natura**	**Strumento**
Comunicazione	Messaggi di posta Elettronica	Client e-mail microsoft
Registri/Repertori	Obblighi di legge (Infortuni, Provvedimenti/ Repertori, …)	Strumentazione elettronica e strumenti diversi
Archivi	Archivi di deposito e storico	Strumenti diversi da quelli elettronici
Notificazioni	Atti del messo notificatore, pubblicazione albi	Strumenti diversi da quelli elettronici
Messaggistica	Server di Posta Elettronica interno	Strumenti elettronici – Microsoft Exchange
Servizi Bibliotecari	Dati personali	Punto di accesso internet, Prenotazioni

10.8 Manuale di Gestione del Protocollo Informatico

Per quanto riguarda la gestione dei documenti in entrata e uscita dall'ente, nonché al trattamento di registrazione, distribuzione e selezione dei documenti con dati si fa espresso riferimento al 'Manuale di gestione del protocollo Informatico redatto ai sensi del DPCM 30.10.2000 che descrive dettagliatamente le modalità di raccolta, registrazione, acquisizione, assegnamento, distribuzione, selezione, blocco dei documenti sia cartacei che digitali dell'ente.

Detto manuale norma le fasi di archiviazione e conservazione e accesso ai documenti e fascicoli documentari contenenti dati personali.

10.9 Documenti informatici

Un sezione specifica riguarda il trattamento dei dati personali contenuti o gestiti in modalità informatica a formare documenti informatici.

Qualsiasi documento che non abbia valore storico o artistico o sul quale il ministero dei beni e delle attività culturali non abbia potere di controllo è conservabile utilizzando la conservazione sostitutiva.
Partendo dalla differenziazione tra documenti analogici ed informatici la procedura da seguire è analoga. Per la conservazione sostitutiva, è necessario che quando si tratti di documento informatico - inteso come rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti - sia apposta la firma digitale. Quando invece si trattano documenti analogici (ad esempio documenti cartacei, cassette, nastri magnetici ecc.) che sono validi indipendentemente dal processo di sottoscrizione che viene applicato, questi potranno essere sottoposti al procedimento di

conservazione in qualsiasi momento previa apposizione della sottoscrizione elettronica anche all'insieme dei documenti.
Il processo di conservazione è regolato dalla delibera del CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) del 19 febbraio 2004.

Per quanto concerne i documenti informatici, questi, anche sottoscritti ed eventualmente le loro impronte, vengono memorizzati su supporti ottici ed il responsabile della conservazione vi appone il riferimento temporale oltre che la firma digitale, dopo aver attestato il coretto svolgimento del processo.

Con il DM del 23 gennaio 2004 si estende il supporto ottico a qualsiasi supporto idoneo a garantire la conformità dei documenti agli originali.

La distruzione dei documenti analogici di cui è obbligatoria la conservazione è consentita soltanto dopo la conclusione della procedura di conservazione digitale.
Un ruolo fondamentale nel procedimento di conservazione è ricoperto dal responsabile della conservazione. Infatti questa figura oltre a definire le caratteristiche ed i requisiti del sistema di conservazione dei documenti, garantisce la corretta conservazione del documento, il suo reperimento e la sua esibizione, verifica la funzionalità del sistema e dei programmi in gestione, adotta le misure necessarie per la sicurezza fisica e logica del sistema, provvede a convocare il pubblico ufficiale qualora si renda necessario, verifica periodicamente la leggibilità dei documenti conservati.

I documenti analogici e i documenti informatici

La normativa prevede un differente trattamento dei documenti a seconda che questi siano analogici o informatici. In linea generale, i documenti informatici hanno bisogno di essere sottoscritti elettronicamente e singolarmente perché possano sostituire a pieno titolo il corrispondente cartaceo.
I documenti analogici, che sono validi indipendentemente dal processo di sottoscrizione e per questo possono essere scansionati e sottoposti al processo di conservazione in qualsiasi momento.

Conservazione dei documenti informatici

La loro conservazione è normata dalla delibera del CNIPA 19 febbraio 2004. La conservazione ha come scopo il mantenimento del documento integro ed autentico nel tempo.
Art. 3: "Conservazione sostitutiva di documenti informatici. - 1. Il processo di conservazione sostitutiva di documenti informatici, anche sottoscritti, così come individuati nell'art. 1, lett. f), ed, eventualmente, anche delle loro impronte, avviene mediante memorizzazione su supporti ottici e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo".

Il DM 23 gennaio 2004, Art. 3 amplia la gamma di supporti utilizzabili per la memorizzazione: non solo, quindi, supporti ottici, ma qualsiasi supporto idoneo.

Conservazione dei documenti analogici

Per i documenti la delibera del CNIPA 19 febbraio 2004 che prevede all'art. 4: "Conservazione sostitutiva di documenti analogici.
1. Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta così il corretto svolgimento del processo.
2. Il processo di conservazione sostitutiva di documenti analogici originali unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine.
3. La distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatto salvo quanto previsto al comma 4 dell'art. 6 del DPR 28 dicembre 2000, n. 445".

Accesso ai documenti informatici
Il diritto di accesso ai dati personali pertanto necessità di azioni organizzative e tecniche che permettano sia l'esercizio ditale diritto, sia da parte del Titolare di poter rispettare i tempi previsti dal Codice. Per quanto riguarda gli aspetti organizzativi una possibile soluzione consiste nell'estensione del sistema informativo di protocollo informatico verso la gestione documentale e la gestione dell'archivio in modo che la centralizzazione di tutti i documenti permetta una agevole accesso tematico.

11 ANALISI DEI RISCHI SUI DATI

11.1 Prospetto sintetico delle norme e degli standard di riferimento

[1] BS7799-2:2002;
[2] ISO/IEC 17799:2000;
[3] ISO 9001:2000;
[4] Linee Guida OCSE/OECD;
[5] ISO/IEC TR 13335 (parti 1, 2, 3, 4, 5);
[6] IT SEC (Applicato in Europa);
[7] ISO/IEC 15408 (Common Criteria – evoluzione ed integrazione dei due precedenti);
[8] Raccomandazione del Consiglio dell'Unione Europea - 95/144/CE - 7 aprile 1995: applicazione dei criteri per la valutazione della sicurezza della tecnologia dell'informazione;
[10] DPR 513/97: regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;
[11] Risoluzione del Consiglio dell'Unione Europea del 6 dicembre 2001: approccio Comune nel settore della sicurezza delle reti e dell'informazione.
[12] Direttiva (denominata direttiva Stanca) 16 gennaio 2002 del Dipartimento per l'innovazione e le tecnologie, sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni;
[13] Direttiva del Ministro Stanca 9 dicembre 2002 "Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali";
[14] D.Lgs. 196/2003;
[15] Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni: "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione", marzo 2004.

11.2 Premessa

La valutazione del rischio si basa sulla combinazione dei fattori:

- rischio intrinseco nel trattamento del dato nonché la sua importanza rispetto alla privacy
- rischio intrinseco negli strumenti che permettono di trattarli

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio sono state suddivise in:

- rischio di area, che dipende dal luogo dove gli strumenti sono ubicati.
- rischio di infrastruttura tecnologica (risorse hardware e software) e rischio di intrusione nelle reti di comunicazione
- rischio legato al fattore umano.

Nella tavola che segue viene riportata una scala crescente del rischio riferita alle varie tipologie di dati trattati:

Tipologia	Rischio
Dati conoscibili da chiunque	BASSO
Dati del personale anche se di natura sensibile	MEDIO
Dati accessibili ai sensi della legge 241/90	MEDIO - ALTO
Dati sensibili	ALTO
Dati giudiziari	ALTO

Il rischio più alto è collegato:

- ai dati 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
- ai dati che costituiscono una risorsa importante per il Titolare, funzionale e tecnologica, in relazione ai danni che deriverebbero da una eventuale perdita

I rischi connessi alla gestione delle banche dati e archivi, intesi quali insiemi di dati anche cartacei che abbiano continuità fisica e logica e per i quali si possa ipotizzare una omogenea esigenza di protezione sono stati classificati e associati ad ogni banca dati.

Tutte le azioni che rientrano tra le misure minime e quelle rapportate al rischio che si corre tendono a salvaguardare:

- la disponibilità
- l'integrità
- l'autenticazione e la riservatezza delle informazioni oggetto di trattamento.

Nella tavola che segue sono riportate le più importanti voci di costo che il Titolare intende contenere mediante l'adozione di un piano di sicurezza realizzato in conformità delle linee guida del presente documento programmatico.

Numero	Causale di Costi tangibili
1	Perdite di materiali (danno fisico)
2	Perdite dovute a non disponibilità delle informazioni
3	Perdite di produttività del personale (non solo ITC) che non produce in parte o del tutto
4	Costi del lavoro e dei materiali per il rilevamento, il contenimento, la riparazione dei danni ai dati
5	Costi per il ripristino delle comunicazioni
6	Costi per il recupero del tempo perduto
7	Eventuale aumento dei premi assicurativi

Altri rischi sono connessi alle qualità dei programmi sia applicativi che i prodotti a pacchetto. Poiché il trattamento dei dati viene eseguito mediante questi programmi, essi debbono soddisfare a determinati requisiti definiti anche dagli standard internazionali di:

- funzionalità
- affidabilità
- usabilità
- efficienza

Per questi aspetti, la contromisura di base è garantita dalle clausole contrattuali laddove prevedono l'assicurazione del servizio di assistenza tecnica applicativa e sistemistica nonché i servizi di manutenzione correttiva e straordinaria dei programmi.

Per quanto riguarda i software a pacchetto, la presenza della licenza registrata, garantisce la possibilità di accesso ai sistemi automatici di aggiornamento dei programmi stessi messi a disposizione dal produttore anche mediante Internet.

Le misure di sicurezza che sono state adottate e quelle che si adotteranno sono finalizzate a ridurre o eliminare i seguenti fattori indesiderati e conseguenze dei rischi.

1	Accesso non autorizzato ai dati personali
2	Interruzione o ritardi dei flussi e processi finanziari
3	Alterazione dei processi amministrativi e contabile
4	Rivendicazioni e/o contenziosi
5	Interruzione procedimenti. Perdita efficienza
6	Ritardi con perdite economiche
7	Violazione della legge sulla protezione dei dati
8	Ricaricamento dei dati e delle informazioni
9	Divulgazione di informazioni riservate con perdita di immagine
10	Interruzione/Alterazione di Pubblico Servizio
11	Danneggiamento al Patrimonio Pubblico

11.3 Piano per la sicurezza

Il presente documento di aggiornamento, contiene le linee guida per la messa a punto e il mantenimento di un piano per la sicurezza che garantisce non solo le misure minime di sicurezza ma soprattutto quelle previste dagli articoli 31 e 32 del D.Lgs. 196/2003.

A tal fine, il Comune adotta un piano per la sicurezza informatica basato su una metodologia specifica.

Il riferimento è alle metodologie accreditate dai recenti standard in materia di sicurezza informatica.

La metodologia applicabile per il raggiungimento degli obiettivi è denominata PDCA (Plan, Do, Check, Act), la quale partendo da una idea di fondo, la sviluppa in modo circolare per verificarne i presupposti stessi. L'acronimo PDCA individua 4 fasi principali:

PLAN	La fase di PLAN consiste nell'identificazione del problema, nella sua analisi, nell'individuazione delle cause reali nonché nella definizione e pianificazione delle azioni correttive
DO	La fase di DO consiste nella preparazione ed applicazione delle azioni pianificate
CHECK	La fase di CHECK consiste nella verifica dei risultati raggiunti a fronte degli obiettivi attesi
ACT	La fase di ACT consiste nel consolidamento dei risultati raggiunti, oppure nell'attivazione di un nuovo ciclo di PDCA, con l'introduzione di opportuni correttivi, se non sono stati raggiunti i risultati attesi

11.3.1 Organizzazione per la sicurezza (Security Organization)

Il Comune dispone di una struttura organizzativa preposta a sovrintendere e controllare i processi e le attività legate alla sicurezza. Nel seguito una descrizione dei processi gestiti.

11.3.2 Classificazione e Controllo delle risorse (Asset Classification and Control)

Il Comune raccoglie e classifica informazioni sulle risorse coinvolte. In particolare le risorse considerate sono:

Sistemi informativi
Sistemi di rete tra le varie sedi (intranet, internet)
Postazioni di lavoro, server, altre attrezzature

11.3.3 Sicurezza del personale (Personnel Security)

Il Comune opera su questo aspetto con i seguenti obiettivi:

Ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture comunali
Accertarsi che il personale addetto sia stato informato sui possibili rischi relativi alla sicurezza delle informazioni

11.3.4 Sicurezza materiale e ambientale (Physical and Environmental Security)

Il Comune opera su questo aspetto con i seguenti obiettivi:

Impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni
Impedire la perdita o il danneggiamento dei dati necessari alla corretta esecuzione dei processi istituzionali
Impedire l'interruzione delle attività

11.3.5 Gestione dei sistemi e delle reti (Computer and Network Management)

Il Comune opera su questo aspetto con i seguenti obiettivi:

Assicurare il corretto e sicuro funzionamento sistemi di elaborazione e delle reti
Minimizzare il rischio di guasti dei sistemi
Proteggere l'integrità del software di base e delle informazioni
Assicurare la disponibilità dei processi di elaborazione dell'informazione e di comunicazione
Garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di rete
Evitare la perdita, modifica o uso improprio delle informazioni scambiate in rete

11.3.6 Controllo degli accessi (System Access Control)

Il Comune opera su questo aspetto con i seguenti obiettivi:

Controllare l'accesso alle informazioni;
Prevenire l'accesso non autorizzato alle informazioni;
Assicurare la protezione dei servizi in rete;
Prevenire l'accesso non autorizzato alle postazioni;
Rilevare attività non autorizzate;
Garantire la sicurezza delle informazioni quando sono utilizzate da eventuali postazioni mobili in rete;
Garantire un adeguato controllo degli accessi ai locali nonché tutto il materiale impiegato.

11.3.7 Sviluppo e manutenzione dei sistemi (System Development and Maintenance)

Il Comune opera su questo aspetto con i seguenti obiettivi:

Garantire che le regole di sicurezza siano realmente attuate nei sistemi informatici in esercizio
Assicurare che la conduzione dei progetti informatici e le relative attività di supporto siano eseguite secondo le regole riportate nel presente piano di sicurezza

Tutti i progetti di nuove applicazioni/servizi sono inseriti nel Piano per la Sicurezza.

11.3.8 Gestione della continuità del servizio (Business Continuity Management)

Gli obiettivi di questa attività sono di contrastare le interruzioni delle attività di servizio e dei processi di servizio critici, causati da malfunzionamenti o da eventuali avvenimenti straordinari. Infatti: "Lo scopo del *Business Continuity Management* è garantire la continuità dei processi dell'Organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni" *(Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni del CNIPA - documento "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" – marzo 2004).*

A fronte delle precedenti considerazioni, in caso di eventuali avvenimenti straordinari, saranno rispettate le seguenti regole:

le procedure applicative, il software di sistema e gli archivi che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente;
il piano d'emergenza deve prevedere il ripristino di tutte le funzioni e non solo i servizi informatici centrali;
per assicurare la continuità dei servizi saranno previste strategie di ripristino più opportune quali:
siti alternativi;
metodi di back up;
sostituzione dei sistemi hardware di elaborazione;
ruoli e responsabilità dei gruppi tecnici di lavoro.

11.3.9 Conformità (Compliance)

Il Comune opera su questo aspetto con i seguenti obiettivi:

Garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari o contrattuali e di qualsiasi requisito di sicurezza;
Garantire il rispetto di tutte le direttive ministeriali e regionali;
Assicurare la conformità dei sistemi con i criteri e gli standard di sicurezza nazionali ed internazionali.

11.4 Strumentazione elettronica

La strumentazione elettronica viene gestita e mantenuta allo stato dell'arte della tecnologia. Il personale è informato sulle linee guida comportamentali al fine di custodia e del mantenimento in efficienza della postazione di lavoro.

11.5 Protezione vulnerabilità altri programmi

La funzionalità dei programmi è garantita dal fornitore sulla base di clausole contrattuali rinnovate di anno in anno. I servizi prestati riguardano la manutenzione correttiva a fronte di variazioni di normativa. I tempi di intervento sono stabiliti.

La protezione degli ambienti software di base dipende dalle modalità con le quali si procede agli aggiornamenti sia mediante iniziative autonome che azioni organizzative e contrattuali che prevedano da parte del fornitore o del produttore la comunicazione anche automatica, dei rilasci di versione a fronte di vulnerabilità note.

11.6 Sistemi di autenticazione

Riguarda la disponibilità del sistema a gestire il sistema di autenticazione dell'incaricato che procede al trattamento dei dati.

Tanto in applicazione delle Regole da 1 a 14 del disciplinare tecnico.

Scheda n. 01		Compilata da	Resp.	Data di compilazione	Marzo 2007
Misura	Modifica password periodica				
Descrizione sintetica	Le credenziali di autenticazione hanno una scadenza (max sei mesi)e tre mesi in caso di trattamento di dati sensibili e sono di lunghezza almeno di 8 caratteri.				
Elementi descrittivi	Il personale è formato al fine di non cedere o comunicare a terzi, la propria password che include anche caratteri non alfabetici (ad esempio simboli di punteggiatura) e un misto di caratteri minuscoli e maiuscoli				
Data aggiornamento:		Marzo 2007			

11.6.1 Modalità di accesso ai dati: Autenticazione utenti sul server

L'accesso al sistema informativo applicativo avviene mediante identificativi le cui regole sono determinate dalla logiche specifiche del software e comunicate dai vari fornitori.

Il responsabile per la sicurezza configura l'ambiente in modo da garantire oltre che la disponibilità anche la riservatezza. La direzione dei S.I. valuta e attua soluzioni specifiche specializzate al governo delle credenziali multiple.

Gli utenti sono dichiarati presso i sistemi server e su questi autenticati e autorizzati. Le credenziali sono configurate in modo da associare le quote disco, le disponibilità di condivisione e di accesso controllato, la durata di validità delle password, la lunghezza o complessità della password stessa.

11.6.2 Modalità di accesso ai dati: Autenticazione utenti sulle postazioni di lavoro

L'utilizzo delle postazioni è comunque visto e strutturato per l'utilizzo in rete e per l'accesso ai dati centralizzati. La parola chiave assegnata è conforme alle disposizioni.

11.7 Modalità di accesso ai dati: Sistema di Autorizzazione utenti

L'ambito di autorizzazione viene rivisto annualmente a cura del responsabile che provvede ad aggiornare il responsabile del sistema. È possibile adottare soluzioni software specifiche. La tecnologia si applica anche ai servizi di teleassistenza da parte dei vari fornitori ai sistemi informativi del Comune..

Scheda n. 02		Compilata da		Data di compilazione	Marzo 2007
Misura	Utilizzo di credenziali per l'accesso alle procedure. Menù personalizzati				
Descrizione sintetica	Le funzioni della strumentazione sono definite e distribuite in relazione agli ambiti del trattamento				
Elementi descrittivi	Le funzioni cui ogni utente è abilitato sono assegnate in funzione delle operazioni che deve compiere				
Data aggiornamento:		Marzo 2007			

11.8 Sistemi Antiintrusione da Virus

La valutazione in ordine alla applicabilità della Regola 16 del disciplinare tecnico.

Il sistema rete è protetto dalle intrusioni da virus mediante una soluzione di impresa che garantisce un automatico aggiornamento centralizzato client/server

Scheda n. 03		Compilata da		Data di compilazione	Marzo 2007
Misura	Antivirus centralizzato con aggiornamento obbligatorio on-line della mappa dei virus.				
Descrizione sintetica	In ogni stazione di lavoro è attivo il controllo su tutti i nuovi file immessi nel sistema.				
Elementi descrittivi	Ogni stazione di lavoro scarica gli aggiornamenti di programma e di definizione dei virus da un server centrale, che a sua volta si tiene costantemente aggiornato al sito del fornitore dell'antivirus				

Scheda n. 04		Compilata da		Data di compilazione	Marzo 2007
Misura	Antivirus server di posta				
Descrizione sintetica	Scansione antivirus sui server POP e SMTP, controllo altri agenti non desiderati (worm, spyware, ...)				
Elementi descrittivi	Ogni messaggio di posta elettronica in transito sui server POP e SMTP viene controllato in base alla definizione dei virus costantemente aggiornata.				
Data aggiornamento:		Marzo 2007			

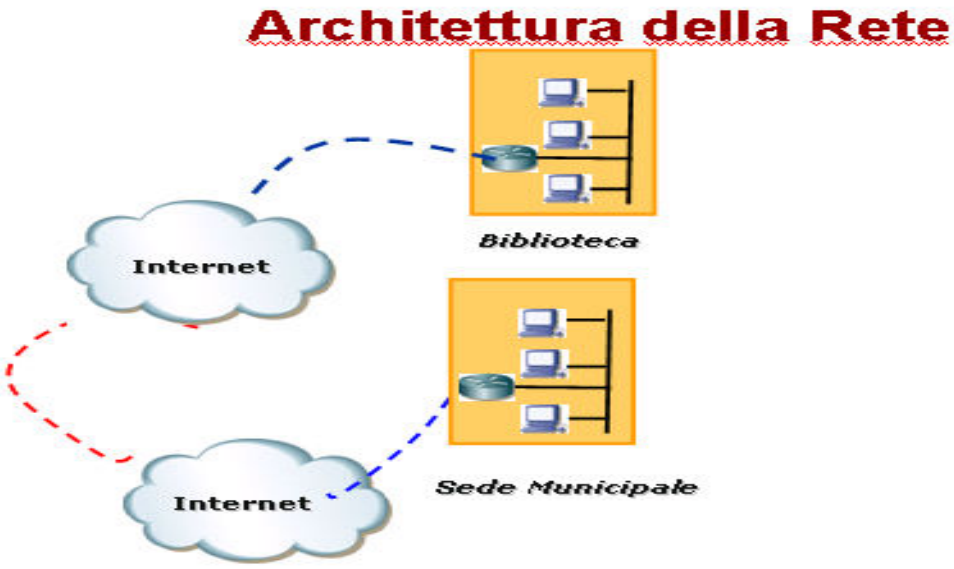
11.8.1 Licenze software

Suite di produttività individuale	Licenze per Device a copertura utenti
Server	Licenze a copertura utenti

11.9 Interconnessione – Sistema di comunicazione

11.9.1 Schema concettuale della rete

Tanto rientra anche nell'applicazione della regola 20 del disciplinare tecnico e qualificata come ulteriore misura in caso di trattamento di dati sensibili e giudiziari: "I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici."



Le componenti di riferimento sono riportate sinteticamente nelle schede che seguono

Scheda n. 05		Compilata da		Data di compilazione	Marzo 2007
Misura	Firewall				
Descrizione sintetica	Predisposizione hardware software per controllare e bloccare l'accesso abusivo dall'esterno e per filtrare l'accesso ai server di database centrali				
Elementi Descrittivi	L'accesso dall'esterno è filtrato al fine di intercettare e bloccare il traffico non necessario e/o non voluto. Il traffico è controllato sia da e verso Internet				

Scheda n. 06		Compilata da		Data di compilazione	Marzo 2007
Misura	Analisi periodica dei log dei firewall				
Descrizione sintetica	I log sono disponibili presso la direzione dei sistemi informativi				
Elementi Descrittivi					

Scheda n. 07		Compilata da		Data di compilazione	Marzo 2007
Misura	Interoperabilità				
Descrizione sintetica	Adozione del sistema più sicuro per la trasmissione/invio di dati				
Elementi Descrittivi Aggiornamento	Modalità di trasmissione con tecniche di cifratura, posta sicura, posta certificata, firma digitale Marzo 2007				

Scheda n. 08		Compilata da		Data di compilazione	Marzo 2007
Misura	Divieto di accesso a mail-box esterne				
Descrizione sintetica					
Elementi Descrittivi Aggiornamento	Gli accessi ad internet sono gestiti anche in modo semantico tramite proxy Marzo 2007				

11.9.2 Altre connessioni

Si tratta di sistemi che consentono ai fornitore di erogare i loro servizi da remoto. I trattamenti riguardano le manutenzioni dei programmi applicativi e dei dati ivi connessi. Per queste attività ci si orienta verso un sistema di concentrazione di tutti i flussi di chiamata.
La strategia di centralizzazione e di controllo delle attività di teleassistenza consente:
un monitoraggio costante
contabilizzazione
ottimizzazione delle attività di amministrazione degli apparati
ottimizzazione delle attività di amministrazione degli accessi
controllo accesso abusivo, il blocco degli accessi
Altre tipologie di comunicazioni riguardano il backbone tra i servizi demografici e il ministero dell'interno per le attività di rilascio della carta di identità elettronica. L'area indicata è soggetta a piani di sicurezza specifici con relative attività di controllo, di gestione dei rischi, di monitoraggio, di comunicazione al Ministero dell'Interno dello stato di mantenimento dei sistemi di sicurezza su quanto riguarda i macroprocessi di acquisizione, gestione, rilascio della carta di identità elettronica.

11.9.3 Disposizioni del Garante

Il Garante per la Protezione dei dati personali con propria deliberazione n. 13 del 1 marzo 2007 ha dettato le linee guida per l'utilizzo della posta elettronica e internet. In particolare:

Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);
c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

1*. Tutela del lavoratore*

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. (2)

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato). (3)

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. *Principi generali*

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (*artt. 1 e 2 del Codice*). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. *Discipline di settore*

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (*artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300*).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (*art. 47, comma 3, lett. b) Codice dell'amministrazione digitale*). [(4)]

2.3. *Principi del Codice*

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del Codice; par. 5.2*);

b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del Codice*). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (*v. par. 3*);

c) i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del Codice: par. 4 e 5*), osservando il principio di *pertinenza* e *non eccedenza* (*par. 6*). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par. 8*) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (Parere n. 8/2001*, cit., punti 5 e 12*).

3. Controlli e correttezza nel trattamento

3.1. *Disciplina interna*

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (*art. 4, secondo comma, Statuto dei lavoratori;allegato VII, par. 3 d.lgs. n. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori"*). [(5)]

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. *Linee guida*

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime –specifiche e non generiche– per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. *Informativa (art. 13 del Codice)*

All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2..

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (*art. 4, secondo comma, l. n. 300/1970*); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.
Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza
Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (*art. 11, comma 1, lett. b), del Codice*), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr. artt. 2086, 2087 e 2104 cod. civ.*).
Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (*art. 4, primo comma, l. 300/1970*), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.
Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli. (6)
In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. É il caso, ad esempio:
- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. (7) A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (*art. 11, comma 2, del Codice*). (8)

5. Programmi che consentono controlli "indiretti"
5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (*art. 4, comma 2*), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. (9) Ciò, anche in presenza di attività di controllo discontinue. (10)
Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati (11), nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. (12)
5.2. *Principio di necessità* In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori *(artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4)*.
Dal punto di vista organizzativo è quindi opportuno che:
- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet; (13)
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure *tecnologiche* volte a minimizzare l'uso di dati identificativi (c.d. *privacy enhancing technologies–PETs*). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).
a) Internet: la navigazione web Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (*art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.*).
In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:
- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);

- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i *file* allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (*artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale*). [(14)]
Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.
La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.
Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").
É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.
In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; (15)
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

6. Pertinenza e non eccedenza

6.1. *Graduazione dei controlli*
Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.
Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.
Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.
Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.
Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.
6.2. *Conservazione*

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla (*v. art. 11, comma 1, lett. e), del Codice*).
Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. *Datori di lavoro privati*

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (*v., in particolare, art. 4, secondo comma, dello Statuto*), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.
Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).
L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. *Datori di lavoro pubblici*

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (*artt. 18-22 e 112*).
In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (*art. 7, comma 4, lett. a), del Codice*).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (*art. 29 del Codice*).
Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.
Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.
Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9).

Alla luce di quanto detto il Garante prescrive quanto segue:

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);

b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:
   - si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
   - si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
   - si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

c) l'adozione di misure di tipo tecnologico, e segnatamente:

   I. rispetto alla "navigazione" in Internet (punto 5.2., a):
      - l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
      - la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
      - il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
      - l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
      - la graduazione dei controlli (punto 6.1.);

   II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):
      - la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
      - l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
      - la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
      - consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
      - l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
      - la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:

   a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;

   b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;

   c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

   d) l'analisi occulta di computer portatili affidati in uso;

4) individua, ai sensi dell'art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

11.9.3.1 Valutazioni

Il Titolare, avvia un procedimento per la messa a punto di un disciplinare interno volto a valutare la possibilità di differenziare i trattamenti personali da quelli del procedimento amministrativo, attivando caselle di posta elettronica istituzionali finalizzate al procedimento amministrativo secondo peraltro le indicazioni già presenti nella normativa (Testo Unico documentazione amministrativa, Codice Amministrazione Digitale, Norme Tecniche e di Gestione della Posta Elettronica certificata).

11.10 Custodia dati personali sensibili e gestione dei supporti

La regola 29 del disciplinare tecnico prevede che l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. L'art. 35 comma 1, lett. c) stabilisce che il titolare prevede procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Scheda n. 9		Compilata da		Data di compilazione	Marzo 2007
Misura	Distruzione fisica dei supporti, formattazione e/o riscrittura				
Descrizione sintetica	Rendere illeggibili le informazioni archiviate su memorie di massa				
Elementi Descrittivi	I dati non necessari contenuti nelle memorie di massa sono resi illeggibili prima della dismissione delle stesse mediante distruzione ovvero mediante formattazione e riscrittura con dati casuali ove la distruzione fisica non sia possibile o particolarmente onerosa				

Scheda n. 10		Compilata da		Data di compilazione	Marzo 2007
Misura	Eliminazione informazioni dalle memorie di massa				
Descrizione sintetica	Cancellazione dei dati del precedente utilizzatore del pc				
Elementi Descrittivi	In caso di riassegnazione di apparecchiature client ad altri utenti, viene assicurata la cancellazione dei dati eventualmente archiviati dall'utente precedente				
Data aggiornamento:	Marzo 2007				

11.11 Sistemi di continuità dell'alimentazione elettrica

L'utilizzo dell'UPS protegge il sistema dei server da eventuali le anomalie della rete di alimentazione elettrica. In particolare, in caso di caduta di tensione l'UPS sostiene il sistema durante la fase di shut-down, garantendo così la correttezza dei dati. I sistemi presenti di potenza adeguata.

Il dispositivo di riferimento è di tipo on-line, ossia sempre attivo e funzionante anche come filtro per l'eliminazione del rumore di varia natura.

Scheda n. 11		Compilata da		Data di compilazione	Marzo 2007
Misura	Uso di gruppi di continuità				
Descrizione sintetica	Alimentazione sostitutiva nel caso di caduta dell'alimentazione di rete				
Elementi Descrittivi	I sistemi di continuità garantiscono la disponibilità di alimentazione elettrica.				
Data aggiornamento:	Marzo 2007				

Il sistema di dispositivi del presente capitolo pur non essendo prescritto in qualità di misura minima, rientra nelle più generali azioni tese ad assicurare il più alto livello di disponibilità dei dati e dei sistemi come previsto dall'art. 31 del nuovo codice.

11.12 I Sistemi Informativi Gestionali

Il sistema informativo svolge le funzioni per le quali è stato installato.

La conduzione e gestione dei servizi ICT è interna. Sono definiti "servizi ICT" per la progettazione, realizzazione, manutenzione, gestione e conduzione operativa di sistemi informativi automatizzati, i servizi denominati "servizi informatici e affini" di cui all'allegato 1, categoria 7 (numero di riferimento della CPC 84) del Decreto Legislativo 17 marzo 1995, n. 157 e s.m. che sono sintetizzati nella tavola che segue:

Consulenza manageriale
Trattamento documentale
Acquisizione di dati
Conduzione funzionale di sistemi informativi Evoluzione sistemi Supporto tecnico agli utenti
Conduzione tecnica di sistemi informativi Esercizio Controllo sistemi
Fornitura di beni hardware e software

Tabella 7 – Servizi ICT

Una parte dei servizi ICT, necessari per garantire la disponibilità sia dei sistemi che del software sono delegate ai vari fornitori, in seguito a specifici contratti di servizio. Si tratta di:

Sviluppo di software applicativo
Rientrano in questo servizio tutte le attività previste nei cicli di vita del software presenti in letteratura: progettazione, disegno, codifica, test; un riferimento è costituito dalla norma ISO/IEC 12207 Information technology – software life cycle processes.

Manutenzione di software applicativo
Manutenzione correttiva, per la rimozione di cause ed effetti dei malfunzionamenti delle procedure e dei programmi; manutenzione adeguativa, per la verifica e adeguamento del sistema informativo alla elevata dinamica della tecnologia (hardware e software di base) che impatta direttamente sul software applicativo; manutenzione migliorativa, finalizzata ad evitare lo scadimento delle prestazioni del sistema informativo coinvolgendo anche programmi e procedure non sottoposti ad interventi correttivi, adeguativi o evolutivi; manutenzione evolutiva, in conseguenza di mutate disposizioni normative e/o regolamenti oggetto di automazione, dell'esigenza del corretto scambio di flussi informativi con altri sistemi informativi esterni, delle mutate esigenze degli utenti, dell'attivazione di ulteriori posti di lavoro o di uffici periferici automatizzati.

11.12.1 Servizi di configurazione del software e nuovi servizi

Il nuovo codice prevede, sia tra i suoi principi che nel contesto della regolamentazione dei diritti del cittadino, quali siano le modalità di trattamento mediante strumenti elettronici. I riferimenti normativi sono i seguenti:
"**Art. 3 (Principio di necessità nel trattamento dei dati**) - I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità";
"**Art. 7 (Diritto di accesso ai dati personali ed altri diritti)** - L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile ….. c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici";
"**Art. 10 (Riscontro all'interessato)** - Per garantire l'effettivo esercizio dei diritti di cui all'art. 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico".

Il Titolare comunque provvede con gli strumenti a disposizione ad agevolare l'esercizio del diritto di accesso ai dati personali. In particolare per quanto riguarda l'art. 10, lett. a), comma 1, il sistema di Protocollo Informatico conforme al DPR 445/2000 potrà agevolare il Titolare nella incombenza di garantire il diritto di accesso ai dati personali da parte dell'interessato.

Inoltre l'art. 22 prevede:

I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

11.12.2 Sistemi informativi automatizzati

Descrizione	Fornitore/Prodotto	Tecnologia Principale
Anagrafe, Stato Civile, Elettorale, Gestione ICI, Contabilità Finanziaria, IVA, Economato, Gestione del Personale, Rilevazione Presenze, Protocollo Informatico, Gestione Delibere, Banca dati UTE	Halley Veneto	Wintel
Gestione delle Pratiche Edilizie, Gestione e calcolo del contributo di concessione, Gestione amministrativa dei Lavori Pubblici	Datapiano	Wintel
WinSIT	Politecnica	Wintel
Gestione del sito web	E-Group	Wintel
Gestione codice della strada	Open software	Wintel

11.13 Modalità di accesso ai dati delle postazioni di lavoro

Scheda n. 11		Compilata da		Data di compilazione	Marzo 2007
Misura	Configurazione delle condivisioni e degli accessi per utenti o gruppi				
Descrizione sintetica	L'accesso "via rete" ai dati presenti su repository centralizzati oppure sui singoli PC è protetto				
Elementi Descrittivi	Il trattamento di alcuni dati può comportare varie fasi svolte spesso da incaricati diversi. Le applicazioni esistenti sono normalmente di tipo client/server				
Data aggiornamento:		Marzo 2007			

11.14 Misure relative al "Rischio di area"

11.14.1 Area sede dei locali del Centro Elaborazione Dati

La sicurezza fisica è applicata con livelli commisurati alla valutazione del rischio specifico e della tipologia e caratteristiche ed ubicazione degli edifici disponibili. I locali del Centro Elaborazione Dati sono protetti in una sala ad accesso controllato. La rete elettrica è a norma con cablaggio su armadio interno per il controllo dell'alimentazione stabilizzata.

Gli impianti ed i sistemi di cui è dotato il Comune sono adeguate e tali mantenute al fine di garantire i livelli di sicurezza attesi.

Le persone che accedono ad archivi contenenti dati sensibili fuori orario sono autorizzati ed identificati. Un apposito registro, consente di registrare e identificare le persone che a vario titolo accedono fuori orario che dovrà essere regolarmente firmato volta per volta.

Scheda n. 12		Compilata da		Data di compilazione	Marzo 2007
Misura	Chiusura locale macchine e accesso selezionato e controllato				
Descrizione sintetica	Il locale dove sono custoditi i server centralizzati è accessibile solo a personale autorizzato				
Elementi Descrittivi	L'accesso è permesso solo a personale autorizzato e abilitato				
Data aggiornamento:		Marzo 2007			

11.14.2 Area sede del Comune

L'accesso agli uffici è controllato dal personale.

11.14.3 Custodia dati personali sensibili

La regola 29 del disciplinare tecnico prevede che l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. L'art. 35, comma 1, lett. c) stabilisce che il titolare prevede procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.
La sicurezza fisica è applicata con livelli commisurati alla valutazione del rischio specifico e della tipologia e caratteristiche ed ubicazione degli edifici disponibili.

11.15 Procedure di sicurezza dei dati

La regola 23 dell'allegato B) Disciplinare Tecnico: "Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.", rientra tra le ulteriori misure da adottare in presenza di dati sensibili e giudiziari.

La tavola che segue riporta schematicamente il contesto in essere:

Scheda n. 13		Compilata da		Data di compilazione	Marzo 2007
Misura	Backup				
Descrizione sintetica	Viene effettuato un backup giornaliero con ricovero dei supporti in locali diversi. Il set della settimana viene conservato Inoltre viene archiviato un set di backup mensile e annuale				
Elementi Descrittivi	giornaliero feriale (da lunedì a venerdì)				

Scheda n. 14		Compilata da		Data di compilazione	Marzo 2007
Misura	Sistemi RAID (Redundant array of inexpensive disks)				
Descrizione sintetica	si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è quella di garantire la disponibilità e l'integrità dei dati, anche nel caso di guasto hardware di uno dei dischi che compongono il sistema				
Elementi Descrittivi	Presenti su tutti i sistemi server				
Data aggiornamento:	Marzo 2007				

11.16 Supporto all'utente

L'utente viene supportato dal responsabile per la sicurezza. Lo scopo è assicurare la disponibilità dei dati finalizzati al trattamento.

11.17 Tavole per l'analisi dei rischi

Nel seguito, le tavole che riportano le misure effettuate e la valutazione del rischio delle banche dati e di seguito sono descritti i vari contesti.

		Impatto sulla sicurezza dei dati		Riferimento a misure d'azione
Risorse Umane	Evento	Descrizione	Gravità stimata	
			Alta Media Bassa	
	Furto di credenziali di autenticazione	Utilizzo di codici utente/password di altro dipendente	Bassa	Utilizzo di file di log e modifica della password a scadenza determinata
	Carenza di consapevolezza, disattenzione o incuria	Abbandono della propria postazione con sessione avviata e applicativi aperti	Media	Utilizzo di salva schermo. Disconnessione per time out. Formazione e sensibilizzazione degli utenti
	Comportamenti sleali o fraudolenti	Utilizzo volutamente errato di applicativi	Bassa	File di log. Utilizzo di credenziali per l'accesso alle procedure. Menù personalizzati
	Errore materiale	Immissione nel sistema di dati errati	Alta	Utilizzo di applicativi con regole di congruenza sui dati immessi. Procedure di backup.
Eventi relativi agli strumenti	Errori di progettazione e sviluppo che consentono accessi non autorizzati o producono malfunzionamenti o comportino il blocco del funzionamento	Immissione nel sistema di dati errati	Alta	Servizi di manutenzione, gestione patch, credenziali di autorizzazione

		Impatto sulla sicurezza dei dati		Riferimento a misure d'azione
Risorse Umane	Evento	Descrizione	Gravità stimata	
			Alta Media Bassa	
	Azione di virus informatici o di codici dannosi	Danneggiamento dei dati applicativi e di sistema del proprio pc	Alta	Antivirus centralizzato con aggiornamento automatico on-line della mappa dei virus. Antivirus su server di posta. Divieto di accesso a mail_box esterne. Backup.
	Spamming o altre tecniche di sabotaggio	Immissione incontrollata e non voluta di posta con degrado della funzionalità del server di posta e delle stazioni di lavoro	Bassa	Utilizzo di filtri anti spamming
	Malfunzionamento, indisponibilità o degrado degli strumenti	Lo stato degli strumenti rende difficile l'attività funzionale	Media	Uso di gruppi di continuità; Interventi da parte di gruppo di assistenza
	Accessi esterni non autorizzati	Utenti esterni possono tentare di inserirsi nella rete al fine di danneggiare o acquisire informazioni	Media	Firewall
	Accessi interni non autorizzati	Personale non autorizzato si collega alla rete da punti rete dell'ente	Alta	Blocco fisico delle porte.

Risorse Umane	Evento	Descrizione	Gravità stimata	
			Alta Media Bassa	
	Accessi da parte di aziende che collaborano con il Comune per la manutenzione degli applicativi	Tecnici delle ditte di assistenza si collegano in remoto alla rete	Medio/Alta	Controllo diretto dell'attività. Protocollo di comportamento.
Intercettazione di informazioni in rete	Intercettazione di informazioni in rete interna	Possibilità di intercettare pacchetti e decodificare utenti e password	Bassa	Modifica periodica password
	Intercettazione di informazioni in rete esterna - Internet	Possibilità di intercettare pacchetti	Bassa	Formazione utenti; Trasmissione in forma criptata.
Banche dati	Accesso non autorizzato			Credenziali di autenticazione
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Danneggiamento fisico attrezzature	Bassa	Chiusura locale macchine e accesso selezionato
	Asportazione e furto di strumenti contenenti dati	Danneggiamento fisico attrezzature	Media	Chiusura dei locali e accesso solo personale autorizzato
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali	Danneggiamento dei supporti	Alta	Backup giornaliero Diversificazione fisica dei locali e siti di conservazione.
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, …)	Danneggiamento attrezzature	Alta	Backup giornaliero Gruppi di continuità
	Errori umani nella gestione della sicurezza fisica	Danneggiamento attrezzature	Alta	Backup giornaliero; formazione del personale

Risorse Umane	Evento	Descrizione	Gravità stimata	
			Alta Media Bassa	
Supporti	Deterioramento Inagibilità del media Evoluzione tecnologica			Backup Riversamento Piano di continuità
	Dismissione di supporti contenenti dati	Possibilità di acquisire informazioni contenuti su supporti dismessi (es. floppy, CD-ROM, HD, USB-pen)	Media	Distruzione fisica dei supporti, formattazione e/o riscrittura dei dischi
	Protezione vulnerabilità determinati programmi informatici	Manutenzione correttiva di sistemi operativi e di software di base e di ambiente	Bassa	Sistemi automatici Patch sistemi operativi diversi, RDBMS, gestionali

Tabella 8 – Analisi rischi

12 MISURE MINIME DI SICUREZZA

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), sono previste delle misure minime da adottare. Nel seguito la descrizione delle misure e le indicazioni degli elementi progettuali per l'eventuale adeguamento o adozione di strumenti per la gestione della sicurezza.

12.1 Sistema di autenticazione informatica

Il sistema di autenticazione informatica ha lo scopo di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato e laddove i dati non siano destinati alla diffusione. Per realizzare le credenziali di autenticazione 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, mantenerla riservata e modificarla periodicamente

12.1.1 Stato attuale

Caratteristica
Il trattamento di dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo
La credenziale di autenticazione in possesso è ad uso esclusivo dell'incaricato
Il sistema operativo consente di differenziare vari livelli di autenticazione per l'accesso con la modalità di amministratore
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri. È modificabile dall'incaricato al primo utilizzo
È modificabile dall'incaricato, almeno ogni sei mesi In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificabile almeno ogni tre mesi.
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivabili
Si verifica la condizione per la quale l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione

12.1.2 Valutazione

Si è in presenza di credenziali multiple assegnate ad ogni persona. Indipendentemente dal fatto che i sistemi operativi e le applicazioni consentano l'aggiornamento, la complicazione gestionale a carico dell'utente, potrebbe inevitabilmente nel tempo portare a comportamenti generali non coerenti con la norma. Si prevede di attivare sistemi di gestione automatica delle credenziali di autenticazione

12.2 Sistema di autorizzazione informatica

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, risulta necessario adottare un sistema di autorizzazione informatica che stabilisce a quali aree dati, quali servizi di trattamento utilizzabili, quali siano le azioni che si possono fare.

L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

12.2.1 Stato attuale

Caratteristica
Ci sono condizioni per le quali il trattamento riguarda solo dati destinati alla diffusione
Si verifica la condizione per individuare profili di autorizzazione di ambito diverso
Esiste un sistema di autorizzazione unico.
I profili di autorizzazione, sono individuati e configurati in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione
I sistemi informativi implementano un sistema di autorizzazione per vari livelli di trattamento (selettivo)
I sistemi informativi implementano un sistema di autorizzazione individuale e di gruppo

12.2.2 Valutazione

Per particolari uffici non appare necessario prevedere profili di autorizzazione distinti, per le diverse persone, in relazione alle limitate dimensioni dell'ufficio stesso, o per il fatto che ragioni organizzative e di continuità del servizio sono assegnate le stesse preposizioni a più persone.

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**.**

È stato adottato un prodotto standard di mercato che estende le misure minime di sicurezza e che gestisce le autorizzazioni all'uso degli strumenti elettronici per:

- utente
- gruppo
- server

Il sistema evolve verso la centralizzazione, consente di amministrare i desktop dalla console dei server e mantiene traccia delle attività.

12.3 Protezione contro il rischio di intrusione

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

Riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui **Art 615-quinquies.** Legge 23 dicembre 1993, n. 547 - ***Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità; informatica***
"(Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico). - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente 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, è; punito con la reclusione sino a due anni e con la multa sino a lire venti milioni".

Questi tipi di programmi sono comunemente conosciuti come virus.

12.3.1 Stato attuale

Caratteristica
È utilizzato un software antivirus nelle modalità necessarie: controllo delle attività sul Personal Computer, controllo dei messaggi di posta elettronica, controllo degli allegati di posta elettronica, controllo delle pagine Internet in ordine a cookies, activex, java
Il sistema è centralizzato e aggiornato automaticamente con frequenza sistematica
L'antivirus in dotazione è in grado di riconoscere virus polimorfici
L'antivirus controlla in automatico ogni file scaricato dalla rete o letto da supporti esterni quali Floppy Disk e CD-ROM
È possibile programmare un controllo approfondito periodico di tutti i file presenti nel sistema
Il personale è informato al fine di evitare l'introduzione di virus informatici nella rete

12.3.2 Valutazione

Si è dotati di idonei strumenti elettronici e programmi, che il D.Lgs. 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto di sottoporre ad aggiornamento con maggiore frequenza. Il responsabile per la sicurezza provvede a garantire il corretto funzionamento del sistema.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Le regole sono applicate in modo migliorativo e superiore ai parametri minimi imposti dalla norma.

12.4 Protezione contro l'accesso abusivo

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

L'aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo. "**Art. 615-ter.** Legge 23 dicembre 1993, n. 547 - **Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità; informatica** - (Accesso abusivo ad un sistema informatico o telematico). - Chiunque abusivamente si introduce 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, è; punito con la reclusione fino a tre anni.La pena è; della reclusione da uno a cinque anni:
1) se il fatto è; commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità; di operatore del sistema;
2) se il colpevole, per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è; palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità; o alla protezione civile o comunque di interesse pubblico, la pena è; rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è; punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

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.

12.4.1 Stato attuale

Caratteristica
Si è dotati di tali strumenti, per la protezione degli elaboratori in rete

12.4.2 Valutazione

La rete è protetta dalle intrusioni dall'esterno. Il sistema garantisce un controllo semantico del traffico, provvede a impedire il download di elementi potenzialmente dannosi amplificando quindi l'azione del sistema antivirus. Periodicamente i flussi relativi ai sistemi antiintrusione sono ruotati e riscritti.

Le regole sono applicate con funzionalità superiori alle imposizioni minime e per il momento sono previsti solo gli interventi di manutenzione e di gestione sulla base delle scadenze temporali stabilite dal D.Lgs. 196/2003.

12.5 Programmi per prevenire la vulnerabilità

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

Si tratta 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.

Nel caso non siano disponibili sistemi automatici, è compito dell'amministratore del sistema provvedere, sotto il controllo del Responsabile per la Sicurezza, anche con procedure non automatiche all'aggiornamento dei sistemi.

12.5.1 Stato attuale

Caratteristica
Si è dotati di tali strumenti, per l'aggiornamento dei sistemi in modo automatico
Esiste una funzione organizzativa che consenta di provvedere in modo pianificato all'aggiornamento in alternativa al sistema automatico
I programmi di utilità e di produttività sono regolarmente licenziati
I programmi di ambiente sono regolarmente licenziati
I sistemi operativi per postazione di lavoro sono regolarmente licenziati
I sistemi operativi per server sono regolarmente licenziati

12.5.2 Valutazione

L'azione in essere, che consiste nel pianificare i sistemi operativi in modo che si provveda all'avviamento del servizio di updating postazione per postazione è ritenuta sufficiente per le dimensioni della struttura.

Si valuta l'implementazione del servizio gratuito S.U.S. di Microsoft al fine di rendere la citata attività completamente automatica. Il servizio predetto richiede una postazione dedicata.

13 GESTIONE DEI SUPPORTI REMOVIBILI

Si tratta di memorie di massa esterne e removibili:

- floppy disk
- CD-ROM
- ZIP
- HD esterni

Altri dispositivi: smart memory, ecc.

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

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

13.1.1 Stato attuale

Caratteristica
Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati dati personali al fine di evitare accessi non autorizzati e trattamenti non consentiti
Esistono supporti rimovibili contenenti dati sensibili o giudiziari non utilizzati
In caso di riutilizzo da altri incaricati, non autorizzati al trattamento degli stessi dati, le informazioni precedentemente contenute sono rese non intelligibili e tecnicamente in alcun modo ricostruibili

13.1.2 Valutazione

In particolare, essi sono conservati in cassetti chiusi a chiave, per il periodo necessario, e successivamente formattati.

Quando è cessato lo scopo per cui i dati debbono mantenersi memorizzati su di essi, ovvero cessate le ragioni per la conservazione, sono posti in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti.

In caso di non utilizzo i supporti sono distrutti.

14 CRITERI E MODALITÀ DI RIPRISTINO DEI DATI

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

L'art. 34, lett. f) prescrive l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

L'art. 61, comma 3, lett. d) del DPR 445/2000 prescrive che il responsabile del servizio cura che le funzionalità del sistema di Protocollo Informatico in caso di guasti o anomalie sia ripristinato entro 24 ore.

La disponibilità dei dati nell'ambito delle misure minime prevede la cadenza delle azioni di copia di sicurezza entro sette giorni.

I documenti cartacei, e gli eventuali supporti diversi da quelli elettronici, contenenti dati personali, sono comunque assoggettati alle norme relative ai servizi archivistici. I documenti fascicolati sono depositati presso l'archivio generale.

14.1.1 Stato attuale

Caratteristica
Le copie di sicurezza sono custodite
Sono salvati anche i sistemi
Sono ripristinabili anche i sistemi
È in fase di stesura il piano di ripristino per assicurare la continuità del servizio
Durata in giorni (profondità storica)del piano di salvataggio.
Frequenza delle attività di backup
Il sistema consente di provvedere anche alla verifica dei dati
Metodologia di verifica: completa
Modalità di backup Sempre di tipo Completo e differenziale

14.1.2 Piano di continuità operativa

Fonte: AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione
"I dati di un sistema sono sottoposti ad una serie di rischi, che ne minacciano continuamente la disponibilità, che possono andare dai mal funzionamenti hardware agli atti di vandalismo, perpetrati da intrusori informatici. È possibile ridurre al minimo gli effetti, spesso disastrosi, di tali eventi, predisponendo una serie di accorgimenti tecnologici, quali, oltre alle tecnologie e procedure di

riversamento già descritte anche ad esempio un *Piano di continuità operativa*, che costituisce la forma più sofisticata di protezione dai rischi.

Il Piano di Continuità Operativa
Il piano di continuità operativa ha lo scopo di garantire la continuità e la disponibilità, degli strumenti e dei dati, in ipotesi di danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali. L'obiettivo del Piano di Continuità Operativa è quello di ripristinare i servizi informatici entro un tempo prestabilito, in funzione dei livelli di servizio attesi, e di rendere minime le perdite causate dall'interruzione dell'attività.
Ciò significa che il Piano di Continuità Operativa non deve essere inteso come misura alternativa, a quelle di prevenzione, ma è un completamento di queste ultime, al fine di :
- garantire la continuità dei principali processi, assicurando l'erogazione dei servizi essenziali
- limitare gli impatti degli eventi a carattere distruttivo sulla posizione finanziaria.

Il Piano di Continuità Operativa si occupa del controllo delle interruzioni di operatività, al fine di prevenirne e minimizzarne l'impatto, individuando un insieme specifico di contromisure di sicurezza, in grado di sostenere le operazioni critiche dell'organizzazione, anche attraverso infrastrutture alternative.
Lo scopo è quello di raggiungere e mantenere un sistema di operazioni che prevenga i rischi e, in caso di accadimento dell'evento distruttivo, ne limiti l'impatto sulla continuità dell'operatività: a tale fine, sarebbe opportuno attivare un processo di sviluppo e mantenimento di specifici piani, che includano misure di identificazione e riduzione del rischio orientate a limitare le conseguenze di un impatto dannoso, e ad assicurare un rapido ripristino delle operazioni essenziali.
Il processo di pianificazione della Continuità Operativa dovrebbe essere visto come un quadro di riferimento per la gestione di più procedure di ripristino, orientate a coprire scenari di impatto differenziati, in relazione ai diversi eventi dannosi: dalla semplice caduta di alimentazione fino agli eventi catastrofici che richiedono un vero e proprio Piano di *disaster recovery*.
La Continuità Operativa è un processo continuo che si articola in attività di analisi, progetto, attuazione e manutenzione di un piano che deve contemplare:
- identificazione e classificazione per priorità di ripristino di processi ed operazioni critici
- determinazione dei potenziali impatti di indisponibilità, rispetto ai diversi scenari di danneggiamento
- identificazione delle responsabilità ed adozione di contromisure tecniche ed organizzative
- documentazione dei processi e delle procedure concordate (di emergenza, di continuità, di ripristino)
- formazione specifica di tutto il personale sui processi e le procedure della Continuità Operativa
- test, manutenzione ed aggiornamento del piano.

La realizzazione del Piano di Continuità Operativa si basa quindi su contromisure, di carattere sia tecnologico che organizzativo, che indicano cosa fare, con quali risorse, e quali procedure seguire in condizioni di emergenza, che rendano il sistema informativo parzialmente o totalmente indisponibile.
I principali *aspetti tecnologici* riguardano:
- il recupero dei supporti di back-up
- il recupero delle transazioni perse
- il Disaster Recovery, nel caso di impatto per evento catastrofico. In questo caso la principale contromisura di carattere tecnologico consiste nel centro di back-up, che può essere realizzato in uno dei seguenti modi:

- predisponendo una struttura tipo *scatola vuota*, di proprietà dell'organizzazione, o di tipo consortile o in service
- raddoppiando il centro ed integrandolo in rete
- creando un centro di recovery che può essere di proprietà dell'organizzazione, o di tipo consortile o in service.

Dovrà inoltre essere predisposta una struttura di commutazione, che in caso di emergenza sia in grado di commutare l'utenza dal sistema principale a quello di back-up.

- I principali *aspetti organizzativi* riguardano la definizione del piano dettagliato di ***chi fa cosa***, dal momento della dichiarazione dello stato di emergenza a tutto il periodo (anche diversi mesi) durante il quale il centro primario potrebbe rimanere fuori servizio. Nulla deve essere lasciato al caso, per cui il piano dovrà comprendere:
- l'assegnazione delle responsabilità individuali
- le procedure di rilevamento e segnalazione
- il Piano di gestione dell'emergenza
- l'organizzazione della ripartenza delle operazioni essenziali (ripartenza automatica)
- il Piano di gestione della comunicazione verso le Direzioni, altre organizzazioni, il pubblico
- corsi di sensibilizzazione e formazione periodici
- la manutenzione del Piano: organizzazione di test regolari e revisioni di tutte le contromisure, le procedure ed i recovery plan.

L'*attività di manutenzione* del piano riveste particolare importanza, per evitare che il sistema stesso divenga rapidamente obsoleto ed inefficace a causa della:
evoluzione tecnologica dei sistemi hardware e software, sia del proprio sistema informativo che, eventualmente, di quello del Centro di Back-up
evoluzione organizzativa e logistica dell' organizzazione
caduta di attenzione delle persone coinvolte
cambiamento delle persone che occupano i ruoli interessati.
Se il piano non segue tempestivamente questi cambiamenti, perde di efficacia in breve tempo; l'unico modo per verificare che la manutenzione sia effettuata in modo adeguato è quello di programmare prove reali, o almeno "di carico".
Si precisa che, nell'ambito delle misure minime di sicurezza, non è in generale previsto l'obbligo di adottare un piano di continuità operativa (salvi casi particolari, in cui la perdita di dati sarebbe di particolare nocumento per le persone cui essi si riferiscono), la cui complessità lo rende per inciso accessibile solo alle organizzazioni di rilevanti dimensioni: anche per esse, in considerazione del fatto che i Piani di Continuità in genere richiedono investimenti significativi, per la loro realizzazione, è importante che essi vengano definiti, tenendo continuamente presente un corretto rapporto costi/benefici, *nei limiti della loro effettiva necessità*."

Si prevedono investimenti per migliorare il livello di servizio e la disponibilità dei dati in relazione all'aumento dei dati e degli accessi e la contemporanea diminuzione delle finestre di tempo disponibili per le operazioni di backup. Il progetto garantisce un livello di disponibilità dei dati significativo e proporzionato alle dimensioni del Comune.

15 LA CUSTODIA E L'ARCHIVIAZIONE DI ATTI, DOCUMENTI E SUPPORTI

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.

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, sono disponibili:

- cassetti con serratura
- armadi chiudibili a chiave 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, in periodi 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.

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

- controllo interno indiretto da parte del personale presente negli uffici,
- l'accesso all'archivio generale è selezionato,
- le persone dipendenti sono autorizzate preventivamente ad accedere agli archivi,
- si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, mediante l'adozione di un modulo appositamente predisposto,
- gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi, che mantengono in memoria le informazioni su chi abbia avuto accesso ed in quale lasso di tempo.

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 soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per il momento, sono quindi previsti gli interventi di manutenzione e di normale reintegro se ricorrente.

16 FORMAZIONE

La formazione in materia di sicurezza è un processo continuo dopo la prima sessione che ha coinvolto tutti i dipendenti. Le sessioni di formazione di manutenzione delle conoscenza e di approfondimento della legge riguardano in particolare:

- 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
- evoluzione e applicazione della norma.

Gli interventi formativi sono programmati in modo da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Argomenti del corso di formazione:

- Introduzione alla sicurezza informatica
- La sicurezza dei sistemi informativi e la privacy
- Sintesi sul D.Lgs. 196/2003, adempimenti, sanzioni
- Disciplinare tecnico, adempimenti, osservazioni
- Documento programmatico per la sicurezza
- Individuazione del sistema da proteggere
- I rischi al sistema informatico e al sistema informativo, protezione dalle intrusioni e virus informatici
- Definizione del livello di sicurezza da garantire
- Le misure di sicurezza
- Verifica periodica
- La sicurezza ed altre norme di riferimento
- Firma digitale (cenni)
- Regole comportamentali da osservare

17 L'AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal D.Lgs. 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 D.Lgs. 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 D.Lgs. 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, il Titolare si riserva di poter esigere che il destinatario rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

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 apposita lettera scritta.

Detto provvedimento è reso necessario per i fornitori che provvedono, mediante collegamenti telematici o con propri incaricati, alla manutenzione dei sistemi informatici e alle banche dati relative ai sistemi informatici forniti.

18 CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il Titolare è tenuto, anche affidando il compito al designato responsabile per la sicurezza, interno od esterno, ad aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Titolare e le persone da questo appositamente incaricate provvedono con frequenza da stabilire, anche con controlli a campione, ad effettuare una o più delle seguenti attività e a relazionare opportunamente:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite
- verificare l'integrità dei dati e delle loro copie di backup
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

Particolari attività periodiche da svolgere:

Descrizione regola del disciplinare tecnico allegato B) del D.Lgs. 196/2003	Cadenza
5. Sistematica verifica del corretto utilizzo delle parole chiave in caso di trattamento di dati sensibili con strumenti elettronici (In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi)	Trimestrale
5. Sistematica verifica del corretto utilizzo delle parole chiave (la parola chiave viene modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi)	Semestrale
14. Periodicamente è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	Annuale
15. Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici	Annuale
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare periodicamente	Semestrale
17. Aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti	Annuale
17. Aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale	Semestrale
18. Sono impartite istruzioni organizzative e tecniche per il salvataggio dei dati	Settimanale

19 DICHIARAZIONI D'IMPEGNO E FIRMA

Il presente documento, redatto entro i termini, viene firmato in calce da:

Comune di Ponte San Nicolò, in qualità di Titolare

Approvato con:

Provvedimento	**Deliberazione di Giunta Comunale**
Numero	**n. 30**
Data	**04.04.2007**
Oggetto	**Documento Programmatico sulla Sicurezza: aggiornamento e nomina responsabili del trattamento dati**

L'originale del presente documento viene custodito presso l'Amministrazione, per essere esibito in caso di controlli.

Nella relazione accompagnatoria del bilancio si riferisce dell'avvenuta redazione del presente documento che costituisce la prima edizione del Documento Programmatico sulla Sicurezza in adempimento del nuovo codice sulla protezione dei dati personali (D.Lgs. 196/2003).

Ponte San Nicolò, 30 marzo 2007

IL SINDACO
Giovanni Gasparin